(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 June 2001 (21.06.2001)

PCT

(10) International Publication Number
WO 01/44968 A2

(51) International Patent Classification[7]: G06F 17/00

(21) International Application Number: PCT/GB00/04585

(22) International Filing Date:
30 November 2000 (30.11.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
9928523.1 2 December 1999 (02.12.1999) GB
0005714.1 9 March 2000 (09.03.2000) GB

(71) Applicant *(for all designated States except US)*: OAKINGTON CORPORATION PLC [GB/GB]; East View, 5 Coles Lane, Oaklington, Cambridge CB4 5BA (GB).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: MILNER, James, Matthew [GB/GB]; 20 Ross Street, Cambridge CB1 3BX (GB). DAWE, Peter, John [GB/GB]; East View, 5 Coles Lane, Oaklington, Cambridge CB4 5BA (GB).

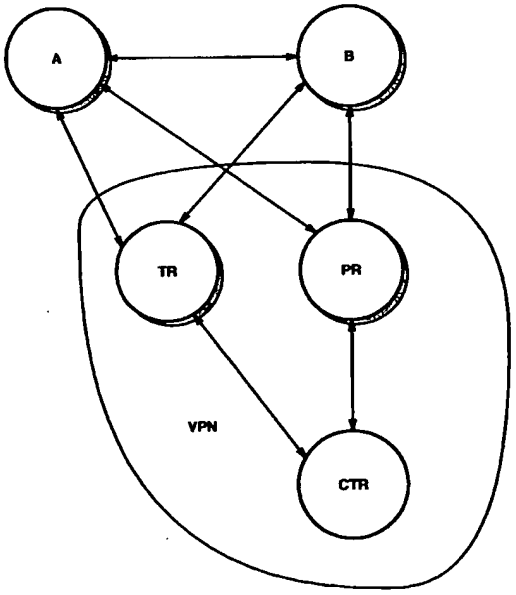
(74) Agents: MUSKER, David, Charles et al.; R.G.C. Jenkins & Co., 26 Caxton Street, London SW1H 0RJ (GB).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: TRANSACTION SYSTEM AND METHOD



(57) Abstract: The invention relates to financial transaction based on notified changes of ownership of statically held tokens. The tokens may be software entities recording data relating to value, value type, expiry date, excrow period and authentication information linking the token to a purse. The purse is an entity which records the existence of the tokens (the tokens being stored on a token server) and is the interface between a user and the token ownership transfer means. The system further includes purse registers which carry data linking the purse with a particular owner. When a token register receives an instruction to transfer ownership of a token, authentication information is forwarded to the purse register where the user is authenticated. The token register may authenticate matters relating to the token itself. The invention is particularly effective in that it prevents the collection of auditing or profiling data for a particular individual.

WO 01/44968 A2

Published:
— *Without international search report and to be republished upon receipt of that report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

TRANSACTION SYSTEM AND METHOD

Field of the Invention

The present invention relates to a system and method for authenticating and/or transferring ownership of tokens. More particularly, but not exclusively, the present invention relates to a system and method for authenticating and/or transferring ownership or digital tokens representing cash, money's worth or other identifier representing intrinsic or extrinsic value.

Background to the Invention

Over recent years many methods of payment for goods and services have been developed. At present times, the majority of small to medium sized transactions are paid for either with cash or using a plastic payment card, such as a credit or debit card. Most of these methods of payments suffer from specific drawbacks however.

In the case of cash, one of the main drawbacks is that if an individual should lose a quantity of cash, unless he is insured, it will generally result in an irretrievable loss of wealth for that individual.

In the case of credit or debit cards, such a card may be fraudulently used if misappropriated merely by imitating the signature of the card holder (as recorded on the reverse side the card), thus fraudulently authenticating the user of the card. Loss or theft of the card may result in fraudulent payments being made until the card is cancelled by the issuing authority.

This problem is accentuated when payments are to be made over a non-secure communications medium such as a public switched telephone network (PSTN) or the Internet. As a consequence, in such situations users are often reluctant to reveal their banking or credit or debit card details, since these may be fraudulently used by a third party who intercepts the communication.

Many known transaction systems aim to provide a secure transaction mechanisms which may be made over networks such as a PSTN or the Internet. Unfortunately, in attempting to do this, the resulting systems invariably become highly complex to operate. This increases the difficulty and expense of using the system, which prevents its widespread establishment.

Examples of such systems range from systems modelled upon debit cards through to digital cash systems. An example of the former type of system is PROTX™ Verified Payment System of PROTX™ Ltd, 38 Belgrave Square, London SW1X 8NT.

In the PROTX™ system, merchants and customers must register with the PROTX™ system as a pre-requisite for making a transaction. In order to purchase an item listed on the website of a merchant, the customer indicates at that site the transaction that he wishes to make. The details of the transaction are then passed to the PROTX™ system. These include the merchant's transaction code and other details of the transaction, such as the price and currency details. The customer is then "passed" to the PROTX™ website, where he is required to authenticate his desire to make the transaction by inputting a user name and password. Once the PROTX™ system has confirmed that the customer is known, the PROTX™ system triggers a payment transfer between conventional bank accounts of the customer and the merchant, via a conventional financial payment mechanism. Finally, the result of the transaction, whether it was successfully completed or not, is communicated to both the merchant and the customer.

Therefore, the PROTX™ system acts as a secure interface between parties wishing to make a transaction over the Internet, and their conventional bank accounts. There are, however, disadvantages associated with such a system. Firstly, the transaction costs associated with the debit card model make it unsuited for low value, very high volume transactions. Such a system is particularly unsuited to transactions in which small payments, such as pennies or cents, or indeed fractions of a penny or a cent are charged. An example of this might be for the sale of information residing on web pages.

Secondly, a complete picture of the financial transactions made by an individual may be generated by systems such as the PROTX™ system. As a result, consumer profiling information relating to individual customers may easily be generated. Consumers may be reluctant to use such systems if they feel that their financial privacy is not assured.

Thirdly, unlike conventional cash, where any person may spend cash that they possess by passing it to any other party, the PROTX™ system only allows money to be

transferred between two parties that are both registered with the PROTX™ system. Thus, unlike the case with conventional cash, for example, only those groups of society with a satisfactory credit rating to obtain a bank account may be able to use systems such as the PROTX™ system. Furthermore, the PROTX™ system only supports the transfer of money to a user that has registered as a merchant. Thus, "peer-to-peer" transactions are not provided for by such systems.

The system operated by DigiCash™ is an example of a digital cash payment system.

The DigiCash™ system aims to overcome the problem of consumer profiling, highlighted above, by ensuring the complete anonymity of a party who spends a DigiCash™ token. When a customer purchases a digital token from a bank, he or she generates a large random serial number, which is "blinded" by another random number. The product is transmitted to the bank, which digitally signs it with a secret key to authenticate it as a new token. The customer then removes the "blinding" factor leaving the true serial number together with the bank's authenticating digital signature. However, the bank does not know the serial number of the token, but merely the "blinded" number and the identity of the customer.

When the token is spent, the recipient of the token presents it to the bank for redemption. The bank recognises the token as authentic due to the presence of its own digital signature, but cannot identify the original purchaser of the token from the token being redeemed.

However, there are certain disadvantages associated with the DigiCash™ system:

Firstly, the bank must retain a record of the serial number of each token which it redeems, in order to ensure that no token is redeemed more than once.

Secondly, DigiCash™ tokens are issued in predetermined denominations, such as $1, or $10. The signature which the bank uses in order to authenticate each token that it issues relies upon Public Key Cryptography techniques. Thus, the bank signs each token with its private key and the signature may subsequently be verified by a recipient of the token using the public key. For each denomination, a separate public key/private key pair is used. This limits the number of denominations of tokens which

may be issued by a bank, since the more public key/private key pairs are used, the easier it becomes for a third party to decipher each key pair (as a result of number field sieve theory). This would make possible the fraudulent minting of further tokens.

Therefore, systems such as DigiCash™ are relatively inflexible in terms of the denominations of token which are available. Consequently, obtaining the correct change for a transaction using DigiCash™ tokens may be difficult or impossible.

Because DigiCash™ is reliant on the computationally intensive process of Public Key Cryptography, it is, like the PROTX™ system, not well suited to low value, very high volume transactions.

Additionally, the anonymity which systems such as DigiCash™ offer makes them attractive vehicles for those engaged with illegal financial activities such as money laundering.

A further example of a digital cash system is NetCash™. Unlike DigiCash™, NetCash™ does not provide purchaser anonymity, thus, reducing the possible application of the system for illegal financial transactions. However, as a consequence the privacy of a user of the NetCash™ system may be compromised since the complete transaction of a given token is known to the token issuing bank.

Additionally, the NetCash™ system, like DigiCash™, uses Public Key Cryptography to authenticate each token, thus rendering it unsuited to low value, very high volume transactions. Again like DigiCash™, a token must be returned to the issuing bank in order that it might be redeemed, where it is removed from circulation. Thus, a large system overhead in generating new tokens is incurred.

Therefore, it would be desirable to provide a transaction system and method which is free from one or more of the above limitations.

Disclosure of the Invention

In one aspect the present invention provides for a method of transferring the ownership of one or more digital tokens, in a financial transaction between two or more parties, each token comprising at least value and ownership data and being stored in a digital token store, the method including the steps of: a first party transmitting, to the token store, data identifying the change of ownership of one or more tokens to a second

party; and, the token store updating the ownership data of the one or more tokens to reflect the transfer of ownership of the one or more tokens to the second party.

In a further aspect, the invention provides for a method of transferring the ownership of a digital token in a digital token transaction system, the token being stored in a token store and the token comprising at least value and ownership data, the ownership data identifying a first device, the method comprising steps of: transmitting an ownership transfer signal from the first device to the token store, the transfer signal identifying a second device; at the token store, modifying the token ownership data in response to the transfer signal so that it refers to the second device.

A signal may be transmitted to the second device confirming the modification of the token ownership data.

A confirmation signal may be transmitted to the first device confirming the modification of the token ownership data.

The token may correspond to electronic cash, shares or other referent having intrinsic or extrinsic value.

In yet another aspect, the invention provides for a method of transferring the ownership of one or more digital tokens in a financial transaction between two or more parties, each token comprising at least value data and ownership data, the ownership data including authentication data, the tokens being stored in a digital token store, the method including the steps of: a first party transmitting, from a corresponding first device to the token store, data instructing a change of ownership of one or more tokens from the first party to a second party; the token store transmitting the authentication data to an authentication means which attempts to authenticate the instruction; and if the instruction is authenticated, the authentication means transmitting a proceed instruction to the digital token store whereby the token store updates the ownership data of the one or more tokens to reflect the transfer of ownership of the one or more tokens to the second party.

The authentication means and digital token store may both be adapted so that information linking the identity of the parties and associated or corresponding devices along with corresponding transaction information cannot be determined from

information held on or interpreted by either the digital token store or the authentication means in isolation.

The authentication means and digital token store are preferably remote from one another.

The method may further include the steps of transmitting a 'request for change' signal from either device to the digital token store; generating and storing a second digital token at the token store, the second token comprising at least value data; incrementing or decrementing the value data of the second token by a value dependent upon the change signal.

The transfer signal may include an escrow period which freezes the value and ownership data of the token for the duration of the escrow period.

The device(s) may comprise a hardware and/or software interface and controlling software.

In yet a further aspect, the present invention provides for a digital token transaction system including: a token database adapted to store a plurality of digital tokens and store ownership data relating to the tokens; one or more token purses adapted to store data identifying one or more tokens stored in the token database, wherein the token database is adapted to receive transaction signals from a first token purse identifying one or more corresponding first tokens stored at the token database and at least one second token purse, the token database being further adapted to modify the ownership data of the one or more first tokens in response to the transaction message so as to associate the one or more first tokens with the at least one second token purse thereby transferring ownership of the one of more first tokens.

The system as hereinbefore defined may further include: a purse database, adapted to store details of purses registered with the transaction system, the purse database being further adapted to receive at least a portion of the transaction message relating to authentication information and to attempt to authenticate the identity of the first purse.

The purse database may be arranged to communicate with the token database over a communications network via encrypted messages.

The system as hereinbefore defined may further include a plurality of purse databases and/or token databases.

The system as hereinbefore defined may further include at least one trust database adapted to store details of the purse and token databases which constitute the digital token transaction system, the trust database being further adapted to generate and/or issue symmetric key pairs used in encrypted communication between components of the token system.

The trust database may be further adapted to communicate with other components of the token system over a communications network, by means of encrypted messages.

The trust database and/or purse database(s) and/or token database(s) may be located on a server, optionally residing on the internet.

The trust database and/or purse database(s) and/or token database(s) may alternatively constitute a virtual private network.

The communications network may be a wide area network, local area network, telecommunications network or similar.

The token purse may comprise software adapted to run on a transaction device.

The transaction device may be a personal computer, palmtop computing device, cellular phone, networked computing device, hardware platform accessible via a network/internet or similar.

The digital token transaction system as hereinbefore defined may further include: an authentication means remote from the token database, the authentication means being adapted to receive authentication data associated with a transaction instruction and to attempt to determine the authenticity of the authentication data, the authentication means being further adapted to transmit an authenticity determination to the token database, whereby the token database is further adapted to, on appropriate authentication, transfer the ownership of a stored token.

The token may correspond to a data string which includes one or more of data relating to ownership, status of the token, escrow period, data identifying the nature of the token value, authentication data identifying the origin of the token, data identifying the hardware on which the token is stored, issue number, validity data, data relating to

permitted uses of the token and data identifying the address of the purse register with which the token is registered.

The token may incorporate a serial number, where the serial number corresponds to the value of the token.

The digital tokens transacted in the system of the present invention are arranged to be held statically on token stores or servers, termed hereafter "token registers", as opposed to being circulated between banks and users, as is the case with conventional cash and prior art digital cash systems based on the conventional cash model, such as DigiCash™ and NetCash™, various important advantages are realised.

Firstly, there is no risk of a token being spent twice by a given individual, as is the case with the system of DigiCash™. Therefore, the operator of the system of the present invention need not retain a list of all tokens which are ever redeemed, as is the case with the system of DigiCash™. Because of this, there is no requirement to encrypt the tokens of the present invention and copies of tokens may be passed to and between electronic purses of the users of the system en-claire. This means that the computationally intensive process of Public Key Cryptography may be avoided, as may be the process of decommissioning tokens after each transaction, followed by reminting new tokens; thus reducing the complexity and cost of the system of the present invention. Similarly, there is no requirement to protect the tokens of the present invention with watermarking or digital signature techniques.

By separating of the tasks of authorising the spending party to a transaction and authorising the value to be transferred in the transaction, using remote or geographically separate servers, "purse registers" and "token registers" respectively, various further important advantages arise.

The first of these is that if a fraudulent third party were to attempt to fraudulently "spend" (or re-assign the ownership) of the tokens of the present invention, it would first be necessary to successfully compromise both the relevant purse register and the relevant token register for the fraud to go unnoticed. Thus, the security of the system is increased over a system in which the two functions are performed by a single entity.

This arrangement of the present invention also allows the system to be easily scaled in order to provide extra system capacity for further users, by the addition of

further purses and tokens. This is because the registers of the present embodiment interact with messaging protocols as is described in the following embodiments. Thus, further purse registers and token registers, which may be used to provide further purses and tokens respectively, may be simply added to a system of the present invention, and their IP addresses made available to the existing servers of the system with which they are to interact. Thus, the number of tokens or purses which may be included in the system of the present invention is limited only by the number of Internet Protocol IP addresses available.

This arrangement of the present invention may be contrasted with the servers of prior art digital cash systems, which store information relating to the ownership of tokens in one database and store information relating to the tokens themselves in a further database linked to the first. In such systems, the speed of operation of the system is dependent upon the size of the databases, thus restricting the scope for scaling such a system. Furthermore, such systems may suffer from dynamic bottlenecks, due to the requirement to manage the interface between the respective databases. Thus, in such systems a certain proportion of spare capacity must be maintained in order to guarantee the smooth operation of the system. This further limits the capacity of such systems.

The ability to handle multiple currencies is essential for e-commerce, where transactions can be international. Due to the separation of the authorisation of the value and the authorisation of the identity of the spending party to a transaction in the system of the present invention, the tokens stored in token registers may be stored in a "notational format", allowing many currencies and securities to be represented by tokens of the present invention. This may be contrasted with prior art, macro-payment digital cash systems, which rely on accounting databases. Such systems can rarely cope with multiple currencies. Furthermore, the protocols of the present invention allow the secure and economic use of the present invention in making both micro and macro-payments.

Additionally, due to the separation of the authorisation of the value and the authorisation of the identity of the spending party to a transaction in the system of the present invention, each purse may communicate with the servers forming part of the system, without requiring encryption techniques. Not only does this reduce the

complexity of the system but it ensures that the speed of operation of the system of the present invention need not be reduced by encryption techniques as is the case with systems such as NetCash™. Furthermore, it ensures that the system may operate across the borders of countries such as the United States, which prohibit the transmission of encrypted data across its boarders.

Further, by ensuring that transfer of ownership of tokens is recorded at the token register and the ownership of a purse is recorded at the purse register, a complete audit trail can be generated for a given token if this is required by the relevant authorities. However, since by virtue of the fact that the two servers are distinct entities, and may indeed be operated by distinct organisations, the privacy of the consumer may be ensured.

By tracking the change in ownership of individual tokens, as opposed to transactions related to a specific individual or related to the purse of an individual, two significant advantages are realised. Firstly, tokens which are under investigation by the police, for example, may be easily tracked forwards and backwards through the economy. Secondly, personal details are not automatically associated with the transaction. This may be used to protect the privacy of users of the present invention.

A further advantage of the present invention is that because the tokens of the system of the present invention are cash equivalents, all sectors of society may use them, not solely those who have a particular credit rating.

The present invention extends to computer programs including code, arranged to perform the methods of the present invention.

Further objects and advantages will be apparent to the skilled reader from the following description and claims.

Brief Description of the Drawings

Specific embodiments of the present invention will now be described by way of example only, with reference to the accompanying drawings, in which:

Figure 1: is a schematic block diagram illustrating the entities making up the system of the first embodiment of the invention;

Figure 2: is a protocol diagram illustrating the in-band procedure for creating a new purse for use with the system of the first embodiment of the invention;

Figure 3: is a diagram of an example of a purse record held by a purse register of the first embodiment of the invention;

Figure 4: is a diagram of an example of a token record held by a token register of the first embodiment of the invention;

Figure 5: is a protocol diagram illustrating the procedure for implementing an instruction to credit in the first embodiment of the invention;

Figure 6: is a protocol diagram illustrating the procedure for implementing an enhanced security credit instruction in the first embodiment of the invention;

Figure 7: is a protocol diagram illustrating the procedure for implementing an instruction to debit in the first embodiment of the invention; and

Figure 8: is a protocol diagram illustrating the procedure for implementing a change operation in the second embodiment of the invention.

First Embodiment

Figure 1 illustrates the entities making up the system of the first embodiment of the present invention. In Figure 1, there are illustrated two "purses", A and B. Each purse is a software program which is designed to store details of digital tokens which are used in the system of the present embodiment to enable users of the system to transact with the digital tokens. Additionally, each purse is arranged to provide an interface for the user, through which he or she may view the value of the coins which are held with that purse and the details of previous transactions.

The software of each purse is stored on and operated by a spending instrument or device (not shown) such as a conventional personal computer, PC, a personal digital assistant, PDA, a smart card or a wireless application protocol, WAP, mobile phone. Irrespective of the type of spending instrument employed to operate a purse, it should be capable of receiving and transmitting information to and from the other elements of the present embodiment, as indicated by the arrows in Figure 1 to enable transactions to occur.

In the system of the present embodiment, any user of the system may hold any number of purses. However, in this example, purse A and purse B are owned by different users (not shown) of the system.

In this embodiment, the communication links between the entities shown in Figure 1 are made over the Internet, however, they may alternatively be made over any other communication network, such as a public switched telephone network or a mobile phone network using a telephone with a data transmission capability, such as GSM mobile telephone network.

Also shown in Figure 1 are three servers: a token register TR; a purse register PR; and, a Central Trust Register CTR, forming a virtual private network. In this embodiment, each of these servers is a conventional server connected to the Internet in a conventional manner.

The purse register PR holds the details of each purse which is registered with it and serves to authenticate each purse which is registered with it as and when that purse is involved in a transaction, as is described more fully below.

The token register TR holds tokens which may be transacted using the system of the present embodiment, together with details associated with each token, such as the identity of the purse which owns it (or is associated with it) and its value. Additionally, the token register TR is arranged to implement transactions between purses of tokens which it holds, as is described more fully below. Thus, in a given transaction, in the system of the present embodiment, the involvement of both the purse register PR and the token register TR are required to authorise the transaction and carry out transfer of value, respectively.

In order to ensure that communications between the purse register PR and the token register TR may not be listened to and interfered with by third parties, their communications are encrypted. In order to reduce delays arising from encryption, symmetric encryption methods are employed, the implementation of which, including the necessary key generation and dissemination, is the responsibility of the central trust register CTR.

As with communications between the token register TR and the purse register PR, communication between the central trust register CTR and both the token register

TR and the purse register PR is protected by symmetric cryptography. Again, the central trust register CTR is responsible for the generation and dissemination of the sessions keys which are to be used.

In this embodiment random numbers are used as the session keys for symmetric encryption and any suitable symmetric encryption algorithms and methods may be used. Examples of suitable symmetric algorithms are Triple-DES and Blowfish, both of which are described in "Applied Cryptography Protocols, Algorithms and Source Code in C", Bruce Schneier, Second Edition, Wiley 1996, ISBN 0-471-12845-7.

New session keys may be distributed using an out-of-band method; i.e. using a data transmission method which does not rely upon a publicly accessible communications channel, for example by post. Alternatively, a suitably implemented communications protocol, such as the Needham Schroeder or the Neuman Stubblebine protocol may be used. These protocols are respectively described in: "Using encryption for authentication in large networks of computers", Communications of the ACM, v.21, n.12, 1978, pp.993-999 and B.C. Neuman & S.Stubblebine "A note on the use of timestamps as nonces" Operating Systems Review, V27, n2, April 1993, pp10-14.

Although Figure 1 shows only a single purse register PR and single token register TR, in practice, the numbers of each of these servers in a system conforming to the present embodiment is unlimited and will be determined by the level of use of the system. In the present embodiment, the number of central trust register is, by contrast, limited to one. However, it is envisaged that in other embodiments more than one central trust register CTR may be employed. This may be useful in the event that the system is very large. In such cases each central trust register CTR may have a geographic jurisdiction, requiring each server of the system in that area to register with it. Alternatively, or additionally, a hierarchical arrangement of central trust registers CTR may be employed.

The central trust register CTR holds a list of all valid servers (purse registers and token registers) within the virtual private network VPN and issues session keys to allow any valid server to communicate securely with any other valid server within the virtual private network VPN. The central trust register CTR is operated by the operator of the system of the present embodiment.

In the event that any server in the virtual private network VPN develops a fault or ceases to operate within the rules laid down by the system operator, the central trust register CTR may deny it access to the system of the present embodiment, by refusing to issue session keys involving that server. Thus, when the session keys which that server is currently using expire, it will be unable to interact with any other server on the virtual private network VPN. However, in the event that it is desirable to halt the activities of a given server in a shorter period of time, the central trust register CTR may send a key revocation message to each server which shares a current session key with that server. Thus, in the present embodiment the central trust register CTR is required to keep a database of all currently active session keys and the servers holding them.

Creating a new purse

A user of the system of the present embodiment may load purse software onto a spending instrument or device, such as an Internet enabled PC as the first step in creating a new purse. It is envisaged that the software for creating a purse will be distributed free of charge and may, for example, be downloaded from the website of the system operator. Because the present embodiment may be implemented without requiring purses to implement any complex encryption processes, the purse software may be relatively simple and so inexpensive to code.

Once the purse software is run by a user, it generates a unique identifier, the "purse identification", which is used to identify the purse. In this embodiment, purse identification is the IP address of the purse. However, as the skilled reader will appreciate, in other embodiments the purse ID may be made up of additional or different information.

The user also obtains the contact details of a purse service provider, which has been approved for use in the present embodiment by the central trust register CTR. The purse service provider is an organisation which operates a purse register such as PR1 in Figure 1. The user also obtains a copy of the central trust register's CTR public key P_{CTR}. It is envisaged that a list of approved purse service providers together with the central trust register's public key may also be obtained from the website of the system operator.

The user then contacts the purse service provider out-of-band, and supplies the purse service provider with personal details and proof of identity and/or residence, as may be required by the purse service provider. In return, the purse register PR1 issues the user with a temporary personal identification number PIN, which is a secure random number, also out-of-band. Preferably, the PIN should be large enough so as to render it probabilistically unique.

The remainder of the procedure for creating a new purse is carried out in-band, and is described below with reference to the protocol diagram illustrated in Figure 2.

At step 1 of the protocol diagram, the user's purse A generates a random secret, termed a subscriber authorisation key $S_{A\text{-}PR1}$, that will be used by the purse registration server PR1 to authenticate all of the spending instruction issued from the purse A. Any suitable method may be used in order to generate $S_{A\text{-}PR1}$. For example, this may be done by timing the key strokes as the user enters his PIN, into his spending instrument when registering his purse (as is explained in Applied Cryptography Protocols, Algorithms and Source Code in C. Bruce Schneier Second Edition, Wiley, 1996, ISBN 0-471-12845-7). The purse A also generates an expiry date ED for the secret $S_{A\text{-}PR1}$.

The purse A then transmits the subscriber authorisation key $S_{A\text{-}PR1}$ to the purse register PR1 in the following manner. The purse A concatenates the PIN, $S_{A\text{-}PR1}$, and the expiry date ED to give a message body of, PIN, $S_{A\text{-}PR1}$, ED. The message body is then encrypted using the central trust register's public key P_{CTR}. The encryption of data X using the public key P_{CTR} is indicated in the following notation by $\{X\}P_{CTR}$. Any suitable assymetric key cryptography protocol may be employed, such as RSA and FAPKC3 (as described in "A new finite automaton public key cryptosystem", T. Renji, C. Shihua, C. Xuemei. Institute of Software, Academia Sinica, Bejing 100080.996.).

This is sent to the purse register PR1 with the user's purse identification A, which is sent en-claire, appended to the encrypted message so that the purse register PR1, which does not possess the central trust register's CTR private key $P^{\wedge}_{CTR}$, may identify the transmitting purse A. Thus the "subscriber authorisation key delivery" message is given by:

1.....$A\{PIN, S_{A\text{-}PR1}, ED\}P_{CTR}$

The skilled reader will appreciate that as the central trust register CTR possesses the central trust register $P^{\wedge}_{CTR}$ but the purse register PR1 does not, it is necessary for the purse register PR1 to transmit the "subscriber authorisation key delivery" message to central trust register CTR for decoding.

Thus, at step two of the protocol, the purse register PR1, having received the user's "subscriber authorisation key delivery" message, further encrypts the entire message using the current symmetric key K_I shared by the purse register PR1 and central trust register CTR and transmits this message to central trust register CTR. The encryption of data X using the a symmetric key K_I is indicated in the following notation by $\{X\}K_I$. Any suitable public/private key cryptography protocol may be employed, such as RSA and FAPKC3 (as described in "A new finite automaton public key cryptosystem", T. Renji, C. Shihua, C. Xuemei. Institute of Software, Academia Sinica, Beijing 100080.996.).

Thus, the "decode subscriber authorisation message" is given by:

2.....$\{A,\{PIN, S_{A\text{-}PR1}, ED\}P_{CTR}\}K_I$

At step three of the protocol, the central trust register CTR returns the PIN, $S_{A\text{-}PR1}$ and ED, to the purse register PR1, having been first decrypted with the symmetric key K_I then decrypted with the central trust register's private key $P^{\wedge}_{CTR}$, and finally re-encrypted with the symmetric key K_I shared between the purse register PR1 and central trust register CTR. Thus the "decoded subscriber authorisation key" message is given by:

3.....$\{A, PIN, S_{A\text{-}PR1}, ED\}K_I$

At step four of the protocol, the purse register PR1 decodes the "decoded subscriber authorisation key" message received from the central trust register CTR and verifies that the PIN is identical to that which the purse register PR1 previously issued to the user out of band. If it is not, then the procedure is aborted.

Otherwise, the purse register PR1 then completes its record of the purse A, which is held at the purse register PR1. This record, an example of which is illustrated in Figure 3 contains the following fields:

The latest PIN issued to a purse by the purse register PR1; PIN The date and time at which the purse was registered with the purse register PR1; the identification

number or code identifying the purse, in the example of the present embodiment the notation used for the identification number of the purse A, is "A"; the identity of the holder (individual or organisation) of the purse; the status of the purse, that is to say whether is currently active or whether is currently "blacklisted" or "frozen" and so unable to effect normal transactions; the current subscriber authorisation key $S_{A\text{-}PR1}$; and, the expiry date ED of the current subscriber authorisation key.

The purse register PR1 then transmits a message to the purse A, confirming that the new subscriber authorisation key $S_{A\text{-}PR1}$ is now valid. This is carried out by sending the PIN and expiry date ED received from the central trust register CTR, encrypted with the new subscriber authorisation key $S_{A\text{-}PR1}$ to the purse A. Thus the "subscriber authorisation key confirmation" message is given by:

4.....$\{PIN, ED\}\ S_{A\text{-}PR1}$

On receipt of this message from the purse register PR1, the user's purse A verifies that the "subscriber authorisation key confirmation" message includes the PIN and expiry date ED matching that transmitted at step 1 of the protocol and confirms the authenticity of the message by decrypting with the subscriber authorisation key $S_{A\text{-}PR1}$.

As the expiry date of the subscriber authorisation key of the purse A approaches, the purse register PR1 issues the owner of the purse A with a new temporary PIN using an out-of-band method, (such as by telephone or post) and a new subscriber authorisation key is generated in the same manner as previously described.

Although in this embodiment the central trust register CTR is used to act as a trusted third party in the process of generating a subscriber authorisation key, the skilled reader will appreciate that any trusted third party might fulfil this role.

Digital Tokens

The tokens which are used in the system of the present embodiment are "minted" on a computer "mint". To increase security, the mint is isolated from public networks and thus is not shown in Figure 1. The newly minted tokens are saved on permanent magnetic media and loaded into a token register TR using a direct fill method. Each token is a digital string made up of various sub-strings, each of which defines a particular attribute of the token.

These include: the "owner's purse ID", defining the purse to which the token currently belongs; the "owner's address", defining the purse register with which the holding purse is registered; the "token register's ID" which identifies the token register holding the token; the "serial number" and "issue number" and the "mint's ID" (identifying the mint which minted the token), which together uniquely define the given token; the "valid from date" and the "expiry date" of the token which jointly define the duration of active life of the token, and which allows the tokens to be retired after a pre-set period; the "token type", i.e. what currency or security the token represents; and, the "token value"; An example of a token record held by the token register is shown in Figure 4.

As has been stated above, the system of the present embodiment is a "notational" system, allowing a great number of different currencies, for example pounds sterling or US dollars, to be represented as different "token types". Furthermore, the "token type" of the system of the present embodiment allows tokens, which represent items of value other than currencies, to be represented. For example, air miles. Indeed, using the system of the present embodiment, any item of worth may be securitised using tokens of the present embodiment. Thus, valid token types may include stocks such as gold, publicly traded shares or any other tradable right such as loyalty/reward points issued by merchants to customers.

In the present embodiment, the initial owner of a given token is the mint. However, on loading the tokens on to the token register, ownership may be transferred to the operator of the token register or a broker. The owner of any registered purse may then purchase tokens of desired denominations on the token register. The operator or broker may, using for example, a secure Internet credit card protocol, such as SET, debit the Visa™ or MasterCard™ of a user of the present embodiment of the invention in payment. The operator or broker then credits him with tokens in exchange. This is achieved using either the basic instruction to credit, enhanced security instruction to credit or instruction to debit as described below.

As and when the owner of a purse wishes to redeem any tokens which it owns, this may be achieved by the above process, in reverse.

Peer-to-Peer Token transactions

In the present embodiment there are three mechanisms for making peer-to-peer transaction with a digital token. That is to say a transaction between two or more purse holders of the system of the present embodiment. Such a transaction may be for example, between two private individuals, two companies, or a company and a private individual. In each case, as explained above either party may be the transferor/payer or transferee/payee. Thus in the case of a transaction between a customer and a merchant, for example, the peer-to-peer transactions described below apply equally to a purchase payment made by the customer to the merchant as a refund made by the merchant to the customer.

In the case of each of the transaction mechanisms of the present embodiment described below, the transactions occur on-line and in real time. Thus, no significant delay due to any clearing process occurs.

In the present embodiment, it is assumed that the party making the transaction is in possession of a token of the correct value for the transaction. Nevertheless, in this embodiment there are two ways in which change for a given token can be obtained.

The first of these is to make a payment with a token of greater value than that required to carry out the transaction and then rely upon the recipient of the token to supply the correct denomination of token in return as change. This may be done in, for example, the case of a merchant providing change to a customer, following the receipt of an initial payment from the customer which was larger than required.

Secondly, a bank, broker or similar organisation operating a "change server" might offer a change service. A change server is simply a purse or a token register containing many tokens of different values of the same currency.

In the present embodiment, the owner of a purse wishing to change tokens of one or more denominations for one or more tokens of further denominations may do so using any of the peer-to-peer payment mechanisms described below by transmitting details of the tokens which are to be changed combined with a message stipulating the number of desired change denominations to the change server.

In addition to changing the tokens, a change server may charge for the service which it provides by returning the change denominations requested, less a fee. The fee

may be based on a percentage of the value changed, or a fixed rate, or any other alternative charging system may be implemented.

For the purposes of the following payment mechanisms described below, the purse A and the purse B are owned by different parties and are registered with different purse registers. However, in practice, they may be owned by the same person and/or may be registered with the same purse register. Furthermore, each may own tokens held on one or more token registers which also holds tokens owned by the other.

The three peer-to-peer payment mechanisms of the present embodiment, an instruction to credit, an enhanced security instruction to credit and, an instruction to debit will now be described below.

Instruction to Credit

Referring to Figure 1, using the instruction to credit, the owner of a purse, the purse A, registered with the purse register PR1 may instruct the payment of one or more tokens owned by it, and held by the token register TR, to a further purse, the purse B, registered with the purse register PR2.

The instruction to credit does not rely upon any direct communication between the transacting parties. Thus, the instruction to credit is useful where there is no requirement or desire for the purse of the payer to be identified by the purse of the payee.

The instruction to credit protocol will now be described with reference to Figure 5.

At step one of the protocol diagram, the purse A transmits to the token register TR an "instruction to credit" message. This message identifies one or more tokens belonging to the purse A, which are held on the token register TR, together with instructions to reassign the ownership of those tokens to a further purse; in this example, the purse B. This message is generated in the following way.

Firstly, the owner of the purse A determines which token or tokens are to be credited to the purse B. In this embodiment, each token is identified in the message sent to the token register TR by its token ID. The token ID is the combination of the contents of three fields of its record held by the token register TR; namely, the "mints unique ID", the "issue number", and the "serial number" (as illustrated in Figure 3),

which jointly serve to uniquely identify any given token. However, the skilled reader will appreciate that any identifier which identifies a token could instead be used. For example the first and last tokens in a contiguous sequence could be used to identity any number of tokens. Alternatively, a complete copy of the digital record of a given token, as held by the token register TR may instead be used.

The token ID of each token which is to be credited to the purse B is concatenated to form what is hereafter termed a summary list SL. The summary list SL is hashed by the purse A, producing a one-way message digest |SL| of the summary list SL. This may be carried out using any suitable, commercially available hashing algorithm such as SHA (as is described in Digital Signature Standard, National Institute of Standards and Technology, NIST FIPS PUB 186, U.S. Department of Commerce, May 1994) or MD5 (as is described in Applied Cryptography Protocols, Algorithms and Source Code in C. Bruce Schneier Second Edition, Wiley, 1996, ISBN 0-471-12845-7) and is carried out using a method known to, and repeatable by, the token register TR.

The purse A then appends to the result of the hash function, |SL|, the identity of the purse A, A, the identity of the recipient purse B, B, and a random number, termed a spending nonce, N_{TR} to form the main body of a message, |SL|, A, B, N_{TR}, to be sent to the token register TR which holds the tokens identified in the summary list SL.

The spending nonce, N_{TR} is a circulating random number generated by the token register and transmitted to the purse A on the completion of the previous transaction. The function of the spending nonce N_{TR} is to ensure that each transaction instigated by the purse A contains a random element, which may not be guessed by a third party. Thus the third party is prevented from "replaying" a previously overheard instruction made by the purse A, to defraud the purse A. Such a method is disclosed in British Patent application 9928523.1, which is hereby incorporated by reference in its entirety. In the case of the first transaction made by the purse A, after being created, a pre-determined spending nonce N_{TR} value is used by the purse A, such as zero. Such a pre-set value will be recognised by the token register TR as the correct value of the spending nonce N_{TR} for use in the first transaction.

The purse A may optionally include in the main message body an escrow period EP and an anonymity flag AF.

The function of the escrow period EP is to place a delay on the spending of tokens received from the purse A by the purse B. This allows the user of the purse A to ascertain whether or not the user of the purse B has complied with his or her obligations associated with the transaction, such as the delivery of goods, before the user of the purse B may use the tokens received. In the event that he or she has not, the user of the purse A may instigate a dispute procedure to reclaim the ownership of the tokens in the escrow.

An escrow period is stipulated by entering a time period following the transaction time and date or an absolute moment in time or other period, in the escrow field of the "instruction to credit" message, corresponding to the end of the escrow period. This field defines an expiry date and time before which no further transaction can take place using that token. The token register then sets up the escrow delay by altering the data held in the "escrow date" field in the record of the relevant token, stored in the token register. If any attempt is made to spend or use the token in any way before the escrow expiry date has been reached, the token register TR will reject the transaction, on checking whether there is an extant escrow period indicated in the "escrow date" field in the record of the relevant token, stored in the token register TR.

The function of the anonymity flag AF is to prevent the recipient of an instruction to credit transaction from being able to identify the purse which made the instruction to credit, as is explained below.

The main body of the message |SLI, A, B, EP, AF, N_{TR} is then signed by the purse A with the secret key $S_{A\text{-}PR1}$, shared between the purse A and the purse register PR1 $S_{A\text{-}PR1}$, which in the following notation is written <|SLI, A, B, EP, AF, N_{TR} > $S_{A\text{-}PR1}$.

The process of signing with a secret is carried out by appending the secret $S_{A\text{-}PR1}$ to the message body and taking a hash of the combination again using a commercially available hashing algorithm such as SHA or MD5. The purse A then sends a message consisting of the original message body |SLI, A, B, EP, AF, N_{TR} without the appended secret $S_{A\text{-}PR1}$, together with the hash formed with the appended secret $S_{A\text{-}PR1}$. The eventual recipient of this message, in this case, purse register PR1, which is also in possession of the shared secret $S_{A\text{-}PR1}$ and the same signing algorithm employed by the purse A, may then carry out the same hashing function; i.e. by appending the shared

secret $S_{A\text{-}PRI}$ to the original message body |SL|, A, B, EP, AF, N_{TR} and taking a hash of the combination and comparing the received hash with that which the recipient generated. If the two hashes match, then the recipient may conclude that the message was sent by a party in possession in the shared secret $S_{A\text{-}PRI}$; i.e. the purse A.

Finally, the summary list SL is appended to the signed portion of the message, unsigned and en-claire, to give the final "instruction to credit message" of:

1.....SL, <|SL|, A, B, EP, AF, N_{TR} > $S_{A\text{-}PRI}$.

The "instruction to credit message" is then transmitted to the token register TR. On receiving the "instruction to credit" message from the purse A, the token register TR carries our the same hashing function as was implemented on SL by the purse A to confirm that the hashed value of SL, |SL|, in the signed portion of the "instruction to credit" message, matches that which it obtains. If a match is not found, the token register TR sends an explanatory error message to the purse A. If a match is found, the token register TR checks that the tokens defined in the summary list SL are indeed owned by the purse A. This is done by matching the identity of the purse A, A, with that found in the "owner's purse ID" field of the records of the tokens indicated in the received summary list, SL. If no match is found for one or more tokens, the token register sends an explanatory error message to the purse A.

Having confirmed that the purse A does indeed own the tokens, the token register TR checks that the spending nonce N_{TR} is current, i.e. that it is the last one it issued to the purse A in order to ensure against a fraudulent replay attack made by a third party. In order to do this, the token register TR must keep a record of the current nonce supplied to each purse owning tokens registered with it. The benefit of carrying out this check is to ensure that a third party eavesdropping on a previous "instruction to credit" transmission sent by the purse A to the token register TR may not be able to fraudulently impersonate the purse A in order to fraudulently replay a spending instruction from the purse A, because the spending nonce N_{TR} it might use will not be current.

When the above checks have successfully been completed, the token register TR checks that the instruction to credit transaction is authorised, as described below, and

then proceeds to generate receipts for the spending the purse A and receiving the purse B.

At step two of the protocol, the token register TR transmits the signed portion only of the "instruction to credit" message, <|SL|, A, B, EP, AF, N_{TR} >$S_{A\text{-}PR1}$, to the purse register PR1 for authorisation of the transaction. The token register TR locates the IP address of the purse register with which the purse A is registered from the "owner's address" field of the record of any one of the tokens included in the summary list SL, as is shown in Figure 4.

However, prior to doing so, it appends a new spending nonce N_{TR}' to the signed message, en-claire and encrypts the entire message, including the new spending nonce N_{TR}' with the current session key, K_1, in use between the token register TR and the purse register PR1. Thus giving the following "check authorisation" message:

2.....{<|SL|, A, B, EP, AF, N_{TR} >$S_{A\text{-}PR1}$, $N_{TR'}$}K_1

On receiving the "check authorisation" message from the token register TR, the purse register PR1 decrypts the message using the current session key K_1. The purse register PR1 subsequently verifies that the secret key $S_{A\text{-}PR1}$ of the purse A was used to generate the "signed with a secret" signature appended to the signed portion of the "check authorisation" message, as described above. However, if the purse register PR1 does not verify that the secret key of the purse A was used to generate the signature an explanatory error message is sent to the token register TR, which is subsequently transmitted to the purse A.

At step three of the protocol, the purse register PR1 responds to the token register TR with a "transaction authorisation" message. This is generated in the following manner.

The purse register PR1 forms a message body consisting of the hashed summary list value, |SL|, the identity of the purse A, A, the identity of the purse B, B, the current nonce N_{TR} and the new nonce $N_{TR'}$, each of which were received from the token register TR in the "check authorisation" message. This message body is hashed with a secret, which is again the purse A's shared secret $S_{A\text{-}PR1}$, to give: <|SL|, A, B, EP, AF, N_{TR}, $N_{TR'}$ >$S_{A\text{-}PR1}$. This is carried in the same manner as described above. The purse register PR1 then transmits this message encrypted with the current session key K_1 shared between

the purse register PR1 and the token register TR, to the token register TR. The "transaction authorisation" message, which forms the basis of a receipt for purse A, as described below, is given by:

3.....$\{<|SL|, A, B, EP, AF, N_{TR}, N_{TR'}>S_{A\text{-}PR1}\}K_1$

Thus, using the authorisation process of the present embodiment, the purse register PR1 is able to confirm to the token register TR that the "instruction to credit" message sent by the purse A to the token register TR, detailing the tokens that the owner of the purse A wishes to transmit to the purse B, did indeed originate from the purse A. This is achieved without the purse register PR1 obtaining any knowledge of the identity or value of those tokens, since the summary list SL transmitted to it in the "check authorisation" message was hashed. Since the hash function is a one way function, even in the event that the purse register PR1 knows which hashing algorithm was used, the token details may not be derived from this knowledge combined with the transmitted hash value.

Thus, the skilled reader will appreciate that the purse register PR1 is unable to record the spending patterns of the purse A. As a result, the information which the purse register PR1 is exposed to, cannot be used in isolation to generate a consumer profile of the owner of the purse A, thus preserving his or her privacy.

Once the token register TR has received the "transaction authorisation" message from the purse register PR1, the transaction is deemed to be authorised and so can proceed. However, in the present embodiment, the token register TR first creates a "generate receipt" message for transmission to the purse register of the purse B. This message forms the basis for a receipt of the credit transaction for the purse B. This is done in the following manner at step four of the protocol diagram.

The token register TR produces a list of the tokens, TL, which are to be credited to the purse B. The purpose of the token list TL is to uniquely identify to the purse B each token which is to be credited to it. Therefore, it contains, as a minimum the same details that were contained within the summary list, SL generated by the purse A in the "instruction to credit" message described above. However, the token list TL may contain up to a complete record of each token as stored in the token register TR.

The token register TR prepares a message body including a hash of the token list |TL|, the identity of the purse A, A, the escrow period used by the purse A in the "instruction to credit" message and a timestamp, T giving the time and date of the generation of the "generate receipt" message.

However, if the purse A introduced an anonymity flag FL in the "instruction to credit" message, the identity of the purse A, A is omitted from this "generate receipt" message. As a consequence, the receipt of the credit transaction which will eventually be transmitted to the purse B will not contain the identity of the purse A and so the purse B will not be informed of the identity of the purse that placed the instruction to credit. Thus, in the "generate receipt" message below, the identity of the purse A which is only included if appropriate is shown as [A].

In the event that the purse A did not include an escrow period in the "instruction to credit" message, a zero or null period will be included in the "generate receipt" message and as well as in the actual receipt that will be transmitted to the purse B.

The token register TR, then transmits the "generate receipt" message body encrypted using the current session key, K_2, shared between the token register TR and the purse register PR2, to the purse register PR2. The "generate receipt" message is given by:

4.....$\{|TL|, [A], B, EP, T\}K_2$

If, at the relevant time, the token register TR and the purse register PR2 do not possess a shared symmetric session key, then the token register TR requests the Central Trust Register central trust register CTR to provide one as discussed above. If, however, a symmetric session key can not be obtained for any reason, then the token register TR will abort the credit transaction and send an explanatory error message to the purse A.

On receipt of the "generate receipt" message, the purse registration server PR2 decrypts the message with its symmetric key pair K_2 and confirms that the identity of the purse B corresponds to a purse registered with it. This is done by searching on the "purse ID" field in the records of purses which are registered with it, as shown in Figure 3.

Having done so, the purse register PR2 generates a hash of the body of the received "generate receipt" message, ⌈TL⌋, [A], B, EP, T, with a secret $S_{B\text{-}PR2}$, shared between the purse register PR2 and the purse B, which is analogous to $S_{A\text{-}PR1}$ shared between the purse register PR1 and the purse A. The hash with secret function is again carried out in the same manner as described with reference to the instruction to credit at step one of this protocol. The purse register PR2 then encrypts the complete "receipt" message with the secret key, K_2, shared between the purse register PR2 and the token register TR, before transmitting it to the token register TR, at step five of the protocol diagram. The "receipt" message for B is thus given by:

5.....$\{<\lceil TL\rfloor, [A], B, T, EP > S_{PR2\text{-}B}\}K_2$

On receiving the "receipt" message from the purse B, the token register TR decrypts it using the appropriate session key K_2.

The token register TR now possessing receipts for both of the transacting purses is able to carry out the transaction by crediting the purse B with the tokens defined by the summary list SL of the instruction to credit transmitted by the purse A.

The transaction is carried out by the token register TR merely by updating the "owners ID" field in the token record stored at the token register TR, for each token involved in the transaction, from the purse A to the purse B.

Thus, as the skilled reader will appreciate, in the present embodiment a transaction involving a given token occurs without that token moving from the token register on which it is stored. Thus, in the present embodiment of the invention, the tokens are static. Because of this, there is no risk of a token being spent twice by a given purse. Thus, the records of tokens which are held on purses registered with the system of the present embodiment, are merely copies of the actual tokens which are stored statically on token registers. Indeed, as has been explained above, the copies of tokens which are stored on the purses may be "cut down" versions of the actual tokens themselves; i.e. they may not include much of the data which goes to make up a token record stored on the token register TR. Although it would result in a less secure system, the present embodiment could be implemented with purses storing nothing but the value of individual tokens stored under their identities at token registers.

The token register TR then adds a timestamp T and the summary list, SL, which it removed at step one of the protocol, to the receipt for the purse A. It also generates and adds a token list TL, corresponding to the summary list, SL, to the receipt for the purse B. Both of the "receipt" messages are then hashed with the secret of the token register TR_{STR} before transmitting the receipts to the purses B and A at steps six and seven of the protocol diagram, respectively.

The "receipt" message for the purse B is given by:

6.....$<TL, <\lceil TL \rfloor, [A], B, EP, T > S_{PR2\text{-}B} > S_{TR}$

The purse B is unable to verify the hash generated with the secret of the token register TR_{STR}. However, by confirming that the receipt has been correctly hashed using its shared subscriber authorisation key, the purse owner may be confident that the transaction has been correctly authorised by the purse register PR2. However, the receipt may be stored by the purse B in the event that the it might be needed at a later date as evidence of the transaction. However, the receipt contains a full description of each of the tokens that the purse B has received from the purse A and now owns.

Purse B may validate the token list TL by hashing it with the secret $S_{B\text{-}PR2}$, shared between the purse register PR2 the purse B and comparing the result with the signed hash $\lceil TL \rfloor$. The purse B may also check the timestamp to deduce that the receipt is "fresh"; i.e. that the receipt is not a copy of a previous receipt which has been accidentally or fraudulently re-transmitted.

However, as has been stated above, the purse identity, A, of the purse A will be missing from the receipt if the owner of the purse A elected to remain anonymous.

The receipt for the purse A is given by:

7.....$<SL, T <\lceil SL \rfloor, A, B, EP, AF, N_{TR}, N_{TR'} >S_{PR1\text{-}A} > S_{TR}$

On receiving the transaction receipt, purse A may verify that the summary list, SL, is unchanged and that the message body of the receipt corresponds to that of the original "introduction to credit" message. However, by confirming that the receipt has been correctly hashed using its shared subscriber authorisation key, the purse owner may be confident that the transaction has been correctly authorised by the purse register PR1. The purse A may also identify the old spending nonce N_{TR} and thus be assured that a receipt is "fresh". The purse A thus concludes that the new spending nonce $N_{TR'}$ is also

"fresh". The new spending nonce N_{TR}' is then saved as the new spending nonce, for use in the next transaction. Like the purse B, the purse A saves this receipt in case it needs to be produced at a later date to authenticate the credit transaction.

By ensuring that purses which are party to a transaction receive receipts from the token register as in the present embodiment, as opposed to from the other party to the transaction as is conventional, a fraud detection mechanism is realised. In the event that a fraudulent third party succeeds in compromising a purse register, such that the purse register validates a faked transaction generated by the third party using the identity of a purse registered with that purse register, the token register nevertheless passes a receipt for the transaction to the defrauded purse. This serves to alert the user of the defrauded purse to the crime.

In such a situation, the owner of the purse may invoke a dispute procedure with the operator of the system, who will be obliged to analyse the transaction records of the tokens of concern to establish whether the dispute procedure has been correctly instigated, and then to take appropriate action.

At the end of each transaction the token register retains a record of the transaction which it has processed. This record, which may be periodically saved onto a permanent storage medium, may be used at a later date to establish an audit trail for a particular token or group of tokens which is under investigation by an authorised authority.

It will be appreciated by the skilled reader that the transaction of the present embodiment clearly separates the respective functions of transferring value between one user of the system and another, carried out by the token register TR and that of authorising that transaction, which is carried out by the purse registers of the purses which are party to the transaction.

As has been explained above, the purse registers are unable to determine how many tokens, or the value of the tokens, which are transacted in any given transaction. Therefore, a party having visibility of a purse register is unable to generate a consumer profile for any given purse, let alone an individual, who may have more than one purse.

Furthermore, although the token register TR is aware of the transfer of value between one purse and another, the token register TR is aware only of the identity of the

purses owning tokens held on that register. Where the owner of a purse holds tokens on more than one token register, as would be the normal case in a mature implementation, any party having visibility of one single token register TR is again unable to generate a consumer profile relating to any given individual.

Furthermore, the token register TR is aware only of the identity of the purses engaged in the transactions and not the details of the owner of any given purse. Therefore, a party having visibility of the token register TR is yet again unable to generate a consumer profile relating to any given individual.

Therefore, in normal circumstances the privacy of each user of the system of the present embodiment is guaranteed.

However, in the event that a relevant authority, such as the police were investigating financial transactions involving one or more particular tokens, the transactions in which those tokens were involved, including the identity of the purses involved and their owners, could be reconstructed by cross referencing transaction records stored in the token register with corresponding purse details held in relevant purse registers.

In the present embodiment, it has been described that the token register TR generates the spending nonce N_{TR} and renews the spending nonce N_{TR}' on each transaction. However, the skilled reader will understand that this role may be incorporated into the functionality of the spending purse instead. Furthermore, it has been described in this embodiment that only one spending nonce is current at any given time. However, the skilled reader will also appreciate that in the event that many transactions are made in rapid succession, more than one spending nonce may be required, in order to avoid the situation where a purse must wait for a first transaction to be completed before being able to enter into a second transaction.

Enhanced Security Instruction to Credit

In the present embodiment of the invention, the owner of the spending purse may choose to use an enhanced security version of the instruction to credit described above.

In the enhanced security instruction to credit protocol of the present embodiment, a symmetric encryption key termed a Purchase Encryption Key, which is

shared by a given purse and a token register on which tokens owned by that purse are held, is used to encrypt messages sent between that purse and that token register.

This gives rise to three security advantages to the owner of the spending purse. By encrypting each communication between the spending purse and the token register with a symmetric key, a third party will not be able to listen in on the communication to gain a picture of the spending profile of that purse.

Furthermore, if the owner of a purse has instructed a token register TR to systematically do so, the token register TR verifies the purchase encryption key of the spending purse, in addition to the purse register PR1 verifying the subscriber authorisation key of the spending purse on each relevant communication. Thus, if a third party were to attempt to fraudulently spend tokens belonging to that purse, they would have to gain knowledge both of that purse's subscriber authorisation key and of its purchase encryption key.

Finally, as is explained below, the token register must, according to the present protocol, confirm with the spending purse that they wish to proceed with the transaction as a penultimate step (i.e. once the transaction is authorised and receipts generated), prior to executing the credit transaction. This strengthens the fraud detection mechanism, described above with reference to the basic instruction to credit protocol, into a fraud prevention mechanism, as is explained below.

In the present embodiment, the purchase encryption key is delivered by a token register to a purse holder out-of-band. However, the skilled reader will realise that a suitable, secure protocol may alternatively be used to deliver it in-band.

The enhanced security credit instruction protocol will now be described, with reference to Figure 6.

This protocol is broadly based upon the instruction to credit protocol. Therefore, similar features and functions will not be described further in detail.

At step 1 of the protocol, the spending purse, purse A, prepares an "instruction to credit" message as has been described with respect to the "instruction to credit" message of the basic instruction to credit protocol. However, this message is transmitted to the token register TR encrypted with a symmetric Purchase Encryption Key $K_{TR\text{-}A}$, shared

by the purse A and the token register TR. The "instruction to credit" message transmitted to the token register TR is thus:

1.....{SL, <|SL|, A, B, AF, EP, N_{TR} > $S_{A\text{-}PR1}$ } $K_{TR\text{-}A}$

The token register TR decrypts the instruction using its symmetric key $K_{TR\text{-}A}$. The token register TR then confirms that the hashed summary list value |SL| in the signed portion of the "instruction to credit" message, matches that which it calculates from the non-hashed value of SL and that the spending nonce N_{TR} is current, as described above with respect to the basic instruction to credit.

At steps 2 and 3 of the protocol, the "check authorisation" message is sent to the purse register PR1 and "transaction authorisation" message is returned to the token register TR by the purse register PR1 in the same manner as described above with respect to the basic instruction to credit protocol. However, in the enhanced security instruction to credit protocol, the token register TR does not send a new spending nonce to the purse register PR1 at step 2 and consequently, a new spending nonce is not returned to the token register TR by the purse register PR1 at step 3.

The "check authorisation" message transmitted to the purse register PR1 at step 2 of the protocol is thus:

2.....{<|SL|, A, B, AF, EP, N_{TR} >$S_{PR1\text{-}A}$}K_1

The "transaction authorisation" message transmitted to the token register TR by the purse register PR1 at step 3 of the protocol is:

3.....{<|SL|, A, B, AF, EP, N_{TR} >$S_{PR1\text{-}A}$}K_1

At steps 4 and 5 of the protocol, a receipt is generated between the token register TR and the purse register PR2 for the receiving purse B in the manner described above with respect to the basic instruction to credit protocol. Thus, the "generate receipt" message transmitted by the token register TR to the purse register PR2 at step 4 of the protocol is:

4.....{|TL|, [A], B, EP, T}K_2

The "receipt" message, for purse B transmitted by the purse register PR2 to the token register TR at step 5 of the protocol is:

5.....{<|TL|, [A], B, EP, T > $S_{PR2\text{-}B}$}K_2

At step 6 of the protocol, once the token register TR has obtained receipts from the purse registers PR1 and PR2, indicating that the token register TR may proceed with the transaction, the token register TR transmits to the purse A a "transaction ready" message. This message contains the old spending nonce N_{TR}, obtained from the records of the current spending nonces of purses owning tokens held by the token register TR, and a new spending nonce N_{TR}', which is newly generated by the token register TR. Both spending nonces N_{TR} and N_{TR}' are encrypted with the purchase encryption key K_{TR-A}. Thus, the "transaction ready" message is given by:

6.....$\{N_{TR}, N_{TR}'\}\ K_{TR-A}$

On receipt of the "transaction ready" message, which it decrypts with its symmetric purchase encryption key K_{TR-A}, the purse A verifies that the old spending nonce, N_{TR}, is the same at that which it included in the original "instruction to credit" message; thus confirming that the "transaction ready" message is fresh. Thus, the new spending nonce N_{TR}' is also deemed to be fresh and, accordingly, is saved as the new spending nonce in the purse A.

Purse A then instructs the token register TR to proceed with the transaction at step 7 of the protocol. This is done by transmitting a "proceed" message to the token register TR, containing the old spending nonce N_{TR}, again encrypted with the purchase encryption key, as shown below:

7.....$\{N_{TR}\}\ K_{TR-A}$

The token register TR decrypts the old spending nonce from the "proceed" message and proceeds with the transaction to which it relates as described above with reference to the basic instruction to credit protocol.

At step 8 of the protocol, the token register TR transmits a receipt to the purse B, in the same manner as described above with regard to the basic instruction to credit. The receipt for purse B is thus given by:

8.....$<TL, <ITLI, [A], B, EP, T > S_{PR2-B} > S_{TR}$

At step 9 of the protocol, the token register TR adds a time stamp to the receipt obtained from the purse register PR1 and hashes the receipt with its own secret S_{TR}, as has been explained with regard to the basic instruction to credit protocol. The token

register TR subsequently encrypts the receipt with the purchase encryption key, prior to transmitting the receipt to the purse A. The receipt for the purse A is given by:

9.....{<SL, <|SL|, A, B, AF, EP, N_{TR} >S_{PR1-A} > S_{TR} } K_{TR-A}

As has been explained above, neither the purse A nor the purse B can verify the hash generated by the secret of the token register TR, but they may store the receipt to authenticate the transaction at a later date should this be required. However, by confirming that the receipt has been correctly hashed using its shared subscriber authorisation key, each purse owner may be confident that the transaction has been correctly authorised by its respective purse register.

Finally, having decrypted the receipt with the purchase encryption key, the purse A verifies that the Summary List SL in the receipt is unchanged from that transmitted on step 1 of the protocol. Purse A also identifies the old spending nonce N_{TR} and is therefore confident that receipt is fresh.

Thus, using the enhanced security instruction to credit protocol, the detection mechanism described with reference to the basic instruction to credit protocol becomes a protection mechanism, since the transaction is not processed by the token register TR until the spending purse has received a receipt from the purse registration servers PR1 and PR2 and then sent an approval message to the token server TR. Thus, the user of the purse A has the option of knowing that the receipts are in order before instructing the token server to proceed with the transaction. Thus, when the present protocol is in operation, a third party attempting to defraud a purse, will inadvertently trigger a receipt for that transaction which requires the approval of the purse holder in order that the transaction is processed.

As mentioned above with respect to the basic instruction to credit, at the end of each transaction the token register retains a record of the transaction which it has processed in order that an audit the token register trail for a particular token or group of tokens may be to established, should this be required.

Instruction to Debit

The instruction to debit is an alternative payment protocol which may be used with the system of the present embodiment. The instruction to debit is suited for use in a situation where one purse is being used to make a payment to a second purse in

exchange for goods or services. However, whereas the instruction to credit was an indirect payment method, the instruction to debit requires communication between the purses party to a transaction. Thus, there is no option for anonymity for the payer purse in the instruction to debit protocol of the present embodiment.

Broadly, speaking, the instruction to debit works in a similar way to the instruction to credit. Therefore, similar processes will not be described further in depth.

The instruction to debit of the present embodiment will now be described with reference to the protocol diagram shown in Figure 7.

At step one of the protocol the purse A generates a message for transmission to the purse B, detailing the tokens whose ownership which is to be transferred from the purse A to the purse B as the payment for a transaction. This message corresponds to the "instruction to credit" message sent by the purse A to the token register TR in the basic instruction to credit protocol, as discussed above, with the exception that there is no option for the purse A to remain anonymous. Therefore, an anonymity flag may not be included in this message. This is because the owner of the purse B will require identification of the purse A in order to know that he has received payment from a particular individual prior to parting with goods or services in return for their payment.

Furthermore, in the instruction to debit protocol, the receiving purse is required to request the appropriate token register, (i.e. the token register or registers storing the tokens which are the subject of the transaction) to re-register those tokens detailed in the summary list, SL under the identity of the purse B. Therefore, it is desirable that purse A includes the IP address of the relevant token register, or registers, in the summary list SL against the respective tokens, as shown, in the "token register's ID" field on the example token record shown in Figure 4.

As was described above with reference to the first step of the basic instruction to credit protocol, this message is sent signed by the shared secret $S_{A\text{-}PR1}$ of the purse A so that it may be authenticated as having originated from the purse A by the purse register PR1. However, it is not encrypted, so that it may be read by the purse B. This allows the user of the purse B to ensure that the transaction details are correct before processing the transaction. Thus, the "tokens to be transferred" message is given by:

1.....SL, <|SL|, A, B, EP, N_{TR} > $S_{A\text{-}PR1}$

Having received the "tokens to be transferred" message from the purse A, the purse B adds its own nonce N_B, en-claire, to the "tokens to be transferred" message received from the purse A and then transmits this whole message to the token register TR as an "instruction to debit" message. Thus, the "instruction to debit" is given by:

2.....N_B, SL, <|SL|, A, B, EP, N_{TR} >$S_{A\text{-}PR1}$

As is described above with respect to the instruction to credit protocol, when the token register TR receives the "instruction to debit" message from the purse B, the token register TR confirms that the hashed value of the summary list |SL| in the signed portion of the "instruction to credit" message, matches that which it calculates from the non-hashed value of the summary list SL and that the spending nonce N_{TR} is current.

The token register TR then proceeds to seek authorisation for the transaction.

At steps three and four indicated in the protocol diagram, a "check authorisation" message is sent from the token register TR to the purse register PR1 of the purse A and a "transaction authorised" message is returned to the token register TR from the purse register PR1. With the exception of the lack of anonymity flag, as has been explained above, the "check authorisation" message and the "transaction authorised" messages conform to steps two and three of the basic instruction to credit transaction described above and so will not be described further. The "check authorisation" message is thus given by:

3.....{<|SL|, A, B, EP, N_{TR} >$S_{A\text{-}PR1}$, $N_{TR'}$}K_1

The "transaction authorised" message is given by:

4.....{<|SL|, A, B, EP, N_{TR}, N_{TR}' >$S_{A\text{-}PR}$}K_1

At step five of the protocol, the token register TR sends a "generate receipt" message to the purse register PR2 in order to generate a receipt of the transaction for the purse B. This message corresponds to the generate received message at step 4 of the instruction to credit protocol. However, in the instruction to debit protocol, the nonce, N_B, received by the token register TR in the "instruction to debit" message from the purse B, is also included in the message in order that it should be included in the receipt which will eventually be passed to B. This is so that the purse B will recognise the receipt as genuine. The "generate receipt" message in the instruction to debit protocol also differs from that of the "basic instruction to credit" message in that it does not

include a time stamp. This is because in the instruction to debit protocol, the transaction was effectively started by the purse B by transmitting the "instruction to debit" message at step 2 of the protocol. Thus the time at which the transaction is completed is of greater interest to the purse B. Hence, a timestamp is included in the receipt for the purse B at a later stage in the protocol, as is described below.

Thus, the "generate receipt" message for the purse B is given by:

5.....$\{<ITL, A, B, EP, N_B\}K_2$

At step six of the protocol the purse register PR2 responds to the "generate receipt" message received from the token register TR at step five of the protocol by sending a "receipt" message to the token register TR. The purse register PR1 carries out the same processes in the present protocol as described in the basic instruction to credit protocol and thus the "receipt" message for the purse B is given by:

6.....$\{<ITL, A, B, EP, N_B > S_{B\text{-}PR2}\}K_2$

The token register then carries out the transaction as described with reference to the basic instruction to credit.

At steps seven and eight of the protocol, respectively, the token register TR transmits the receipts received from the purse registers PR1 and PR2, to the purses A and B, respectively. Generally this is carried out in the same manner as described in the basic instruction to credit protocol. However, the token register TR adds a time stamp T to the receipt for delivery to the purse B for the reasons described above, prior to hashing with the secret of the token register TR_{STR}.

Thus, the receipts for the purse B is given by:

7.....$<TL, <ITL, A, B, EP, N_B > S_{B\text{-}PR2}, T > S_{TR}$

The token register also adds a timestamp to the receipt for the purse A giving the time of the transaction before hashing the messaging with the server S_{TR} of the token register TR. This is useful for the purse A since, the purse A has no control over the time when the purse B chooses to transmit the "instruction to debit" message of step 2 of the protocol.

The receipt for the purse A is given by:

8.....$<SL, <ISLI, A, B, EP, N_{TR}, N_{TR}' >S_{PR1\text{-}A}, T > S_{TR}$

As described above with regard to the instruction to credit protocols, by confirming that the receipt has been correctly hashed using its shared subscriber authorisation key, each purse owner may be confident that the transaction has been correctly authorised by its respective purse register.

The instruction to debit protocol has various advantages for the receiving party, the user of the purse B in the above example, over the instruction to credit protocols.

The first of these is that the recipient is presented with the initial transaction details from the spending party before the transaction is processed. Therefore, the receiving party has the opportunity to request the spending party to correct any errors in the transaction before it is processed.

Secondly, the receiving party may store a number of instructions to debit, potentially from various spending parties, and process them all together in a batch, when it best suits him.

Thirdly, as the recipient of the transaction sends the instruction to debit to the token register TR and subsequently receives a time stamp receipt notifying him of the completion of the transaction, the receiving party has a better guarantee of "freshness" using the instruction to debit than would be the case if an instruction to credit were used.

As mentioned above with respect to the basic instruction to credit, at the end of each transaction using the instruction to debit, the token register TR retains a record of the transaction which it has processed in order that an audit trail for a particular token or group of tokens may be to established, should this be required.

In the present embodiment, in each of the example transactions described, each of the tokens transacted in a given transaction is held on the same token register. If the user of the system wishes to make a payment using tokens held on two or more token registers, this may be done by making a separate transaction for each set of tokens held on a separate token register. In this case each transaction may be carried out in any of the ways described above.

Second Embodiment

The second embodiment of the invention is arranged to carry out each of the functions described above with respect to the first embodiment. Therefore similar apparatus and processes will not be described further in detail.

However, whereas in the first embodiment a user of the system may use a change server or rely upon another user, such as a merchant, to supply the change which he desires, in the present embodiment, a user may generate their own change, as is described below with reference to the protocol diagram shown in Figure 8.

At step 1 of the change protocol, the purse A transmits a request for change, termed a "change request" message to its purse register PR1.

In the "change request" message, the purse A includes the identity of the purse A and the token ID (as described above) of one or two tokens, S_1 or S_1 and S_2, owned in the name of the purse A. In first example below, the case where the token ID of two tokens, S_1 and S_2 are included in the "change request" message will be described. In the second example below, the case where the token ID of a single token, S_1 is included in the "change request" message will be described. In either case, however, each token ID should be sufficient for the token register TR, on which the tokens S_1 and S_2 are stored, to identify the tokens S_1 and S_2, as was described with reference to the first embodiment.

Turning now to the case where the token ID of two tokens, S_1 and S_2 are included in the "change request" message, the "change request" message also includes: the data from the "token register's ID" field of the records of tokens S_1 and S_2, or equivalent identifying information, so that the token register TR holding tokens S_1 and S_2 can be located by the purse registration server of the purse A; the desired "change" values V_1 and V_2 of the tokens S_1 and S_2 when; and, a nonce N_A. As previously described, the nonce N_A serves to ensure that the purse A may be able to identify which change request any change receipts received relate to.

The request is then signed with the secret subscriber authorisation key $S_{A\text{-}PR1}$ which is shared by the purse A and the purse register PR1, prior to being transmitted to the purse register PR1. Thus the "change request" message is given by

1.....$<A, TR, S_1, [S_2], V_1, V_2, N_A, >$

On receipt of the "change request" message, the purse register PR1 establishes that the message was signed with the shared secrete $S_{A\text{-}PRI}$ of the purse A, in so doing confirms that the purse A was the originator of the message. The purse register PR1 then removes the address of the token register TR from the message. The message is then encrypted with the current session key, K_1 shared between the purse register PR1 and the token register TR and transmitted to the token register TR at step 2. The relayed "change request" message is thus given by:

2.....$\{A, S_1, [S_2], V_1, V_2, N_A\}\ K_1$

The "change request" message above shows S_2 in brackets since it may optionally be left out of the "change request" message as described above.

At step 3 of the protocol, the token register TR verifies that the purse A is recorded as the owner of the tokens (S_1, S_2) specified in the relayed "change request" message. This is done in the same manner as described above with respect to the first embodiment. Additionally, the token register TR verifies that $V_1 + V_2$ equals $S_1 + S_2$.

If one or both of these requirements is not complied with, the token register TR sends an explanatory error message to the purse register PR1, which in turn relays it to the purse A.

However, if these requirements are satisfied, the token register TR then changes the value of S_1, S_2 to equal that the specified values of V_1 and V_2, respectively. This is achieved by amending the value data held in the "value" field of the records of the tokens S_1 and S_2 stored on the token register TR and shown in Figure 4, to equal V_1 and V_2, respectively; thus giving rise to "change tokens" T_1, T_2, respectively.

The token register TR then compiles a confirmatory "tokens changed" message to return to the purse register PR1. The message consists of the identity of the purse A, A, the new details of the revalued tokens T_1, T_2, a time stamp, T, giving the date and time that the change was generated and the nonce of the purse A, N_A. The details of the revalued tokens T_1, T_2 may constitute as a minimum, the token ID of those tokens (as discussed in the first embodiment), together with their new values. Alternatively, they may constitute additional information from the token register record shown in Figure 4, up to the full record stored for those tokens.

The message is then encrypted with the current session key K_1 shared between the token register TR and the purse register PR1. Thus, the relayed "tokens changed" message is given by:

3.....$\{A, T_1, T_2, T, N_A\}K_1$

At step 4 of the protocol, the purse register PR1 decrypts the "token changed" message received from the token register TR1 with current session key K_1 the and then relays it to the purse A signed with the subscriber authorisation key $S_{A\text{-}PR1}$ shared between the purse register PR1 and the purse A. Thus, the relayed "tokens changed" message is given by:

4.....$\{<A, T_1, T_2, T, N_A > S_{A\text{-}PR1}$

On receipt of this "tokens changed" message from the purse register PR1, the purse A establishes that it was signed with the secret key $S_{A\text{-}PR1}$ and confirms that the nonce N_A is the same as that issued at step 1 of the protocol; thus verifying the authenticity of the revalued tokens T_1, T_2.

Turning now to the case where the token ID of a single token, S_1 is included in the "change request" message.

In the present embodiment, the token register TR stores not only tokens with a positive value, but also tokens with zero value. These zero value tokens are minted and loaded into the token register TR in the present embodiment in a similar way to that described in the first embodiment with respect to tokens which have a positive value. In the present embodiment, change denominations may be issued in exchange for a single token held by a purse, through the allocation of change to such zero value tokens.

If the token register receives a relayed "change request" message which does not contain a second token ID the token register TR obtains a further token from the number of zero valued tokens stored on the token register TR. The process of providing change then occurs, as described above, by dividing the value of the token S_1, as stipulated by the purse A in the "change request" message between the token S_1/T_1 and the zero value token/T_2. The token register then provides details of the tokens T_1 and T_2, as described above, to the purse register PR1, having updated the "owner's purse ID" field of the token T_2 to show that the token T_2 is now owned by the purse A.

In other respects, the changing process for providing change for a single token is the same as described above with respect to providing change using two tokens. In particular, the skilled reader will appreciate that irrespective of whether the purse requesting the change transmits the token ID of one or two tokens, the token register TR nevertheless carries out the checks described above; namely that the purse A owns the specified token or tokens, as the case may be, and that value is not created or destroyed in making the change.

Although this embodiment describes the "change request" message generated by a purse being routed via its purse register to the appropriate token server, the skilled reader will appreciate that in practice, the purse may transmit the request for change directly to the appropriate token server. Similarly, the "tokens changed" message may be transmitted from the token server directly to the purse.

The skilled reader will appreciate that although the above examples describe the value of one or two tokens being changed to give two change tokens, this mechanism could be used to modify the value of any number of tokens, by changing them to give a greater, lesser or equal number of change tokens. Thus, the mechanism described could be used in reverse, where a user wishes to rationalise his tokens, particularly where they are of low value, by changing two or more tokens for a smaller number of tokens of a higher average value. In this case one or more zero value tokens would be formed, the ownership of which would normally be assigned to the token register operator or similar organisation.

The skilled reader will appreciate that the zero value tokens stored on the token register TR are effectively dormant until such time as value is assigned to them. Therefore, until that time, fields in their token record stored in the token register dependent upon ownership information may be left blank, or may refer to a purse owned by the system operator, or token server operator, for example. Furthermore, until value is assigned to them, there is no necessity for them to have various details such as a serial number assigned to them. Such details may be created by the token register when value is to be assigned to them.

The skilled reader will also appreciate that in the system of the present embodiment, a maximum value for tokens may be fixed by the operator of the system so

that no token may be worth more than a predetermined amount. Thus allowing the operator of the system increased control over the system and in particular allowing the operator increased control to reduce the incentive for fraudulent third parties to commit fraud.

The skilled reader will also appreciate that the changing process described in the present embodiment may be contingent upon the payment of a charge by the purse requesting change to the token register TR_t as discussed with regard to the first embodiment.

The skilled reader will also appreciate that in the system of the present embodiment that the changing process may be implemented by the token server in a manner which is transparent to the user. That is to say, a user may implement an instruction to credit or debit to a value, which does not specify the actual tokens which are to be transacted with. Furthermore, the specified transaction value, although less than the total value of the tokens held by that token register under the identity of that purse, may not equal a whole number of those tokens. In such a case, the token register may automatically change selected tokens which it holds under the identity of that purse to give the transaction value, for use in the transaction, and a change value which is stored under the identity of the spending purse. In such a transaction, the spending purse may instead of sending a summary list of the tokens which are to be used in the transaction, together with a hash of the summary list, in the instruction to credit or debit message, may send a transaction value and the type of token to be used (for example US dollars), together with a hash of this information.

Other Embodiments

It will be clear from the foregoing that the above described embodiments are merely examples of how the invention may be put into effect. Many other alternatives will be apparent to the skilled person which are within the scope of the present invention, some example of which are given below.

Proxy Purse

The skilled reader will understand that although the above embodiments rely upon purse software being run upon a spending instrument which the user of the purse has direct control over, in practice, a "proxy" purse may also or instead be used. A

proxy purse is a server containing one or more purses and their contents. A proxy purse may have at least two elements. The first element is a user interface such as a web page on a web server, which allows the user to interact with the proxy purse. The second element is a set of one or more purses, each of which provides the functionality of a normal purse in carrying out transactions.

The web page should preferably allow a user to view the total value of tokens which he or she holds, their individual values and indicate the escrow period outstanding on any escrowed tokens. It should preferably also provide an interface to allow security checks using a PIN. The purse proxy should preferably also maintain a log of all transactions undertaken by it on behalf of the user.

Having a proxy purse instead of, or as well as having a normal purse may allow a user to make transactions when he or she cannot use his or her normal purse because of physical separation or malfunction, for example. This may be done using a spending instrument such a mobile phone, a PDA or a borrowed personal computer connected via a suitable communications network to access the proxy purse.

Since the spending instruments for use with a proxy purse may be no more than a web browser, for example a WAP phone, or a textual interface such as a GSM phone with a short messaging capability, or any other messaging medium, communications between the spending instrument and the proxy purse, including instructions for transactions may be sent en-claire, without a signature or a nonce.

Instructions for purchases from a merchant with an Internet on-line presence may be sent via the web page of the merchant. The order details may include the identity of the proxy purse service provider used by the customer, the user's proxy purse address and account details.

The merchant may then contact the proxy purse service provider and inform the proxy purse service provider of the details of the transaction which the user has requested. For each order, the merchant may also send to the proxy purse service provider the details of the currency, the value and description of the item, the user's proxy purse identification number, the purse identification number of the merchant and the name of the person who placed the order.

When the user of the proxy purse next contacts the proxy purse service provider, the proxy purse service provider may transmit to the user a list of items waiting to be authorised. However, this may alternatively be sent immediately. The user may then choose to authorise or reject each item on the list. The skilled reader will understand that this should preferably be done using an encrypted instruction, so that it is not open to fraudulent abuse.

In practice, this may be implemented in the following way. The proxy purse service provider may supply the user with a unique (or at least a very high probability of being unique) random number associated with each item waiting to be authorised. The user may then authorise the proxy purse to proceed with the transaction for that item by encrypting the associated random number with a secret shared between the user and the proxy purse, using any suitable encryption protocol.

On receipt of the authorisation instructions, the proxy purse service provider confirms the user's identity by successfully decrypting the message and validating the authenticating message by virtue of the decrypted unique number. The proxy purse service provider may then proceed to carry out the authorised transaction using either a credit or debit instruction as described above.

Reconstructing a Purse

The skilled reader will also appreciate that in the event that a user of an embodiment of the present invention loses his or her spending instrument or the data held in the purse, the purse may be reconstructed. One method of reconstructing a purse is described below.

A user may send his or her purse identity and a nonce to the purse register with which the lost purse was registered. The skilled reader will appreciate that if the purse is lost or destroyed, the user may not be in possession of the his or her subscriber authorisation key, shared between his or her purse and the purse register. In this case, he or she would have to contact the purse register out-of-band to authenticate him or herself.

The purse register, then requests a list of all the tokens that are owned by a purse of the given identity, from all the token registers that the given purse transacted with. The list of relevant token registers is obtained from records of transaction authorisations

previously given to token registers, as described in the first embodiment i.e. it is a list of stored Internet protocol addresses corresponding to those token registers with which that purse has interacted. This list is held at the purse register as part of the transaction records held, as described in respect of the first embodiment.

Each of the token registers with which the given purse has interacted generates a list of the tokens owned by that purse by searching on the "owner's ID" field on each token record for a purse identity matching that in question. Once each token register with which the given purse has interacted has responded to the purse register with a list of tokens owned by that purse, the purse register constructs a full token list of all tokens owned by that purse and sends this list to the owner of the purse in question. Again, this may occur out-of-band. The skilled reader will also appreciate that this procedure may be used if the owner of a purse wishes to check that the data held in his or her purse is in agreement with that held on the system of an embodiment in the present invention.

Transaction Taxation

The skilled reader will also appreciate that the operator of a system according to the present invention may use the system to make charges for its use, or to levy a tax on transactions made using the system, such as is described in British Patent application number 9701997.0 (Published reference GB 2316213 A) which is incorporated herein by reference in its entirety. For example, whenever the ownership of a token is transferred at a token register a charge may be levied for the registration process. This may be implemented simply by decrementing the value of the token held in the "value" field in the token record held at the token register. The decremented value may be credited to an account held by the operator of the system as a usage charge, to an account held a taxation authority as a taxation. The amount decremented may be a flat rate or a percentage of the value of the token, or any other suitable charging or taxing regime may be implemented.

The skilled reader will understand that various other alternatives will be apparent to the skilled person which are within the scope of the present invention.

For example, whereas in the second embodiment, each token was identified by a serial number and has a value which may increase or decrease, as value is transferred between tokens, as users of the system carry out changing processes, the skilled person

will realise that other types of token structure may be used in combination with the system of the present invention. For example, in a preferred embodiment, the serial number may correspond directly with the value of the token. In such a case, each serial number may represent a fixed value. For example, there may exist tokens 1 to 10,000 each representing £1.00. The total value in token register is therefore £10,000 and only adjacent tokens can be aggregated when token ownership is reassigned.

Furthermore, although the above described embodiments are not dependent upon the use of the specific hardware, but instead rely upon general hardware such as personal computers running specific software, the skilled reader will understand that the present invention could instead be implemented using specific hardware, connectable, for example, directly into conventional telephone sockets.

Although the above embodiments are implemented using specific messaging protocols, the skilled reader will appreciate that the present invention could alternatively be implemented using conventional communication protocols. These might include a Secure Socket Layer (SSL), a Transmission Control Protocol (TCP) or a User Datagram Protocol UDP implementation.

Although in the above described embodiments the servers forming a part of the virtual private network communicate over the Internet, the skilled reader will appreciate that they could equally be arranged to communicate over a Local Area Network or a Wide Area Network, or other suitable communications network.

The skilled reader will understand that tokens may also be transacted off-line in a system of the present invention; i.e. without the transaction being authorised by a purse register or the change in ownership being recorded by a token register. Such off-line transactions may be useful if connection to the virtual private network of the present invention is temporarily impossible and/or if the transferor is trusted by transferee, and/or if the risk of payment default is worth taking. For example, if the value of the transaction is very small, then the cost of authenticating the transaction may outweigh, to a significant extent, the transaction value on average. For example, it is now common to find "honesty payment boxes" at news agents where customers are encouraged to pay, unsupervised, for newspapers which are available for self-service purchase.

The skilled reader will also appreciate that the central currency issuers in the present invention may set parameters to ensure that tokens may not be circulated so rapidly as to impede the generation of an audit trail. This may be done using an automatic minimum escrow period, implemented in the same manner as described above with regard to the escrow period described in the first embodiment, for example. Furthermore, the speed of circulation may be regulated according to the value of each token. Thus, a token with a value of £100,000 may be restricted to a daily transfer, whereas a token of a value of £1 may be transferable every 5 minutes.

Furthermore, the skilled reader will appreciate that although in the above described embodiments each purse which is to interact with the system of the invention must be registered, the level of security of such registrations may vary. The level of security may vary dependent upon the number and types of identification which the user provides the operator of the purse register when registering a purse, whether a credit check is submitted to, and the resulting credit rating, for example. This level of security may be reflected in the record of that purse, stored by its purse register and/or the tokens which it owns. Thus users may choose whether or not to transact with other users on the basis of the level of security of that user.

Furthermore, the skilled reader will realise that the system of the present invention could also be used to limit the ways in which a particular type of token, be it representing cash or a different form of security, could be transacted. For example, the token could incorporate data in a field identifying the permitted use of that unit. Such a code would be recognisable to purses of users of the system and the servers of the operator. Thus, redemption or exchange of such units may be prevented unless it is for a particular predetermined good or service obtainable from particular points of sale equipped with a specially programmed and registered purse. Such a system could be used to ensure that pocket money or an allowance given to a child could only be spent at points of sale which sells exclusively goods or services deemed suitable for children.

The skilled reader will appreciate that the system of the present embodiment could be implemented to allow either party to a transaction to use encryption of messages between the transacting purses and/or between the purses and the virtual private network of the system. Any suitable commercially available encryption protocol

may be used, such as those discussed above. This may be agreed on-line or off-line prior to the commencement of the transaction. Such an option may be useful in the event that the transaction is one of very high value.

Various functions may also be incorporated into purses for use with embodiments of the present invention. Such functions may be especially useful in increasing the security with which the purse operates. For example, purses may be protected by passwords or other security system, such as a biometrics scanner. Additionally, purses may be arranged to make payments only to purses pre-specified by the user of the purse.

CLAIMS:

1. A method of transferring the ownership of one or more digital tokens, in a financial transaction between two or more parties, each token comprising at least value and ownership data and being stored in a digital token store, the method including the steps of:

a first party transmitting, to the token store, data identifying the change of ownership of one or more tokens to a second party; and,

the token store updating the ownership data of the one or more tokens to reflect the transfer of ownership of the one or more tokens to the second party.

2. A method of transferring the ownership of a digital token in a digital token transaction system, the token being stored in a token store and the token comprising at least value and ownership data, the ownership data identifying a first device, the method comprising steps of:

transmitting an ownership transfer signal from the first device to the token store, the transfer signal identifying a second device;

at the token store, modifying the token ownership data in response to the transfer signal so that it refers to the second device.

3. A method according to claim 2 further comprising the step of transmitting a signal to the second device confirming the modification of the token ownership data.

4. A method according to claim 2 further comprising the step of transmitting a confirmation signal to the first device confirming the modification of the token ownership data.

5. A method according to claim 2, wherein the token corresponds to electronic cash, shares or other referent having intrinsic or extrinsic value.

6. A method of transferring the ownership of one or more digital tokens in a financial transaction between two or more parties, each token comprising at least value data and ownership data, the ownership data including authentication data, the tokens being stored in a digital token store, the method including the steps of:

a first party transmitting, from a corresponding first device to the token store, data instructing a change of ownership of one or more tokens from the first party to a second party;

the token store transmitting the authentication data to an authentication means which attempts to authenticate the instruction; and

if the instruction is authenticated, the authentication means transmitting a proceed instruction to the digital token store whereby the token store updates the ownership data of the one or more tokens to reflect the transfer of ownership of the one or more tokens to the second party.

7. A method of transferring the ownership of one or more digital tokens as claimed in claim 6 wherein the authentication information passed to the authentication means is hashed thereby allowing the authentication means to authenticate the information without being able to derive any meaningful information itself from the authentication information.

8. A method of transferring ownership of one or more digital tokens as claimed in claim 6 wherein the authentication means and digital token store are both adapted so that information linking the identity of the parties and associated or corresponding devices along with corresponding transaction information cannot be determined from information held on or interpreted by either the digital token store or the authentication means in isolation.

9. A method of transferring ownership of one or more digital tokens as claimed in claim 6 wherein the authentication means and digital token store are remote from one another.

10. A method of transferring ownership of one or more digital tokens as claimed in claim 6 including the further steps of transmitting a 'request for change' signal from either device to the digital token store;

generating and storing a second digital token at the token store, the second token comprising at least value data;

incrementing or decrementing the value data of the second token by a value dependent upon the change signal.

11. A method of transferring ownership of one or more digital tokens as claimed in claim 6 wherein the transfer signal includes an escrow period which freezes the value and ownership data of the token for the duration of the escrow period.

12. A method as claimed in claim 2 where the device(s) comprise a hardware and/or software interface and controlling software.

13. A digital token transaction system including:

a token database adapted to store a plurality of digital tokens and store ownership data relating to the tokens;

one or more token purses adapted to store data identifying one or more tokens stored in the token database, wherein the token database is adapted to receive transaction signals from a first token purse identifying one or more corresponding first tokens stored at the token database and at least one second token purse, the token database being further adapted to modify the ownership data of the one or more first tokens in response to the transaction message so as to associate the one or more first tokens with the at least one second token purse thereby transferring ownership of the one of more first tokens.

14. A digital token transaction system as claimed in claim 13 further including:

a purse database, adapted to store details of purses registered with the transaction system, the purse database being further adapted to receive at least a portion of the

transaction message relating to authentication information and to attempt to authenticate the identity of the first purse.

15. A digital token transaction system as claimed in claim 13 wherein the purse database is arranged to communicate with the token database over a communications network via encrypted messages.

16. A digital token transaction system as claimed in claim 13 further including a plurality of purse databases and/or token databases.

17. A digital token transaction system as claimed in claim 13 further including at least one trust database adapted to store details of the purse and token databases which constitute the digital token transaction system, the trust database being further adapted to generate and/or issue symmetric key pairs used in encrypted communication between components of the token system.

18. A digital token transaction system as claimed in claim 17 wherein the trust database is further adapted to communicate with other components of the token system over a communications network, by means of encrypted messages.

19. A digital token transaction system as claimed in claim 17 wherein the trust database and/or purse database(s) and/or token database(s) is/are located on a server, optionally residing on the internet.

20. A digital token transaction system as claimed in claim 15 wherein the trust database and/or purse database(s) and/or token database(s) constitute a virtual private network.

21. A digital token transaction system as claimed in claim 15 wherein the communications network is a wide area network, local area network, telecommunications network or similar.

22. A digital token transaction system as claimed in claim 15 wherein a token purse comprises software adapted to run on a transaction device.

23. A digital token transaction system as claimed in claim 22 wherein the transaction device is a personal computer, palmtop computing device, cellular phone, networked computing device, hardware platform accessible via a network/internet or similar.

24. A digital token transaction system as claimed in claim 13 further including:

an authentication means remote from the token database, the authentication means being adapted to receive authentication data associated with a transaction instruction and to attempt to determine the authenticity of the authentication data, the authentication means being further adapted to transmit an authenticity determination to the token database, whereby the token database is further adapted to, on appropriate authentication, transfer the ownership of a stored token.

25. A method as claimed in claim 1 wherein the token corresponds to a data string which includes one or more of data relating to ownership, status of the token, escrow period, data identifying the nature of the token value, authentication data identifying the origin of the token, data identifying the hardware on which the token is stored, issue number, validity data, data relating to permitted uses of the token and data identifying the address of the purse register with which the token is registered.

26. A method as claimed in claim 1 wherein the token incorporates a serial number, where the serial number corresponds to the value of the token.

27. A system as claimed in claim 13 wherein the token corresponds to a data string which includes any one or more of data relating to ownership, status of the token, escrow period, data identifying the nature of the token value, authentication data

identifying the origin of the token, data identifying the hardware on which the token is stored, issue number, validity data, data relating to permitted uses of the token and data identifying the address of the purse register with which the token is registered.

28. A system as claimed in claim 13 wherein the token incorporates a serial number, where the serial number corresponds to the value of the token.

29. A method of transferring the ownership of one or more digital tokens as claimed in claim 6 wherein the change of ownership instruction is sent directly to the token register from the first device and the authentication information is sent directly to the authentication means from the first device.

30. A method of transferring the ownership of one or more digital tokens, in a financial transaction between two or more parties substantially as described herein and with reference to the drawings.

31. A digital token transaction system substantially as described herein and with reference to the drawings.

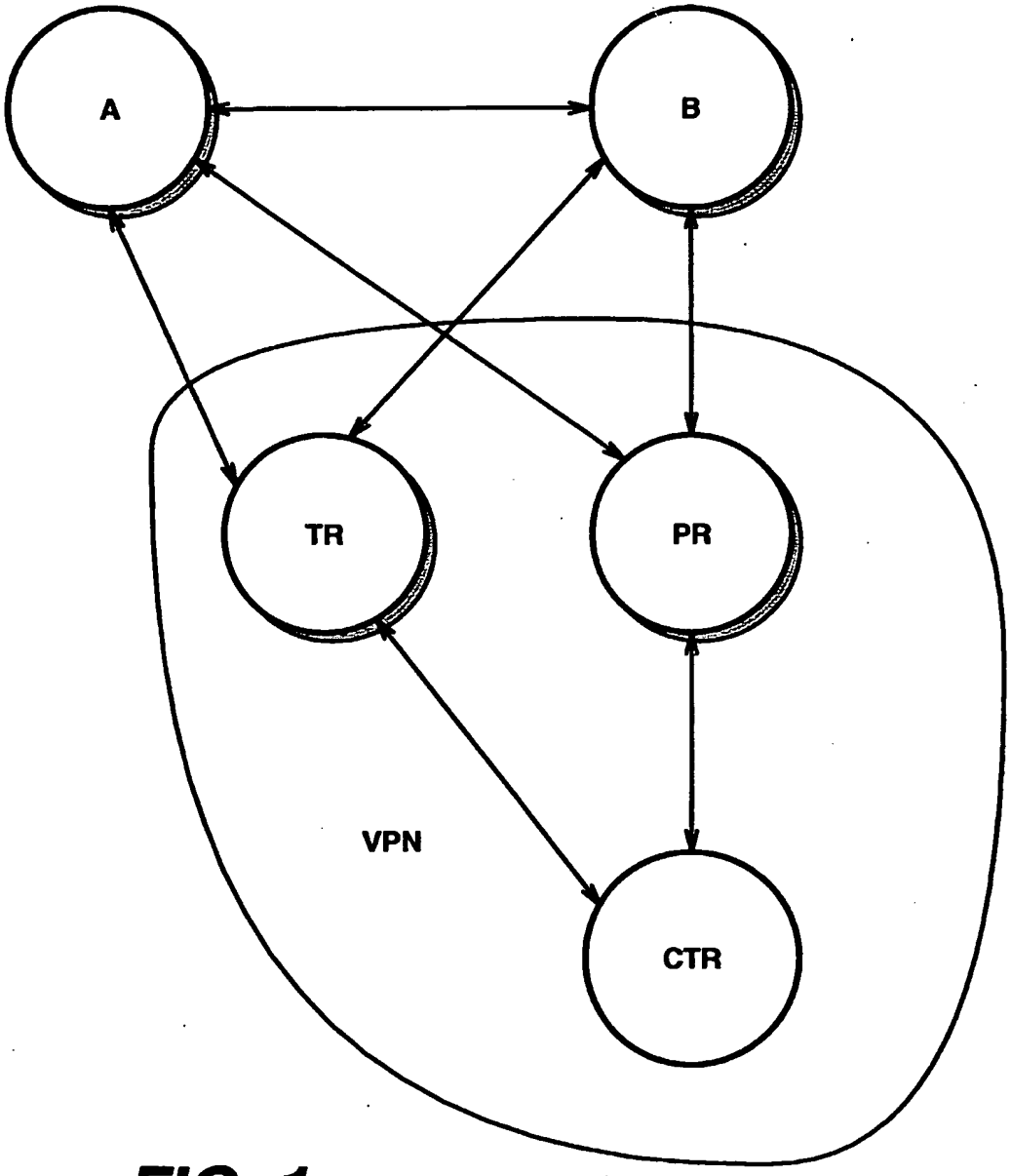


FIG. 1

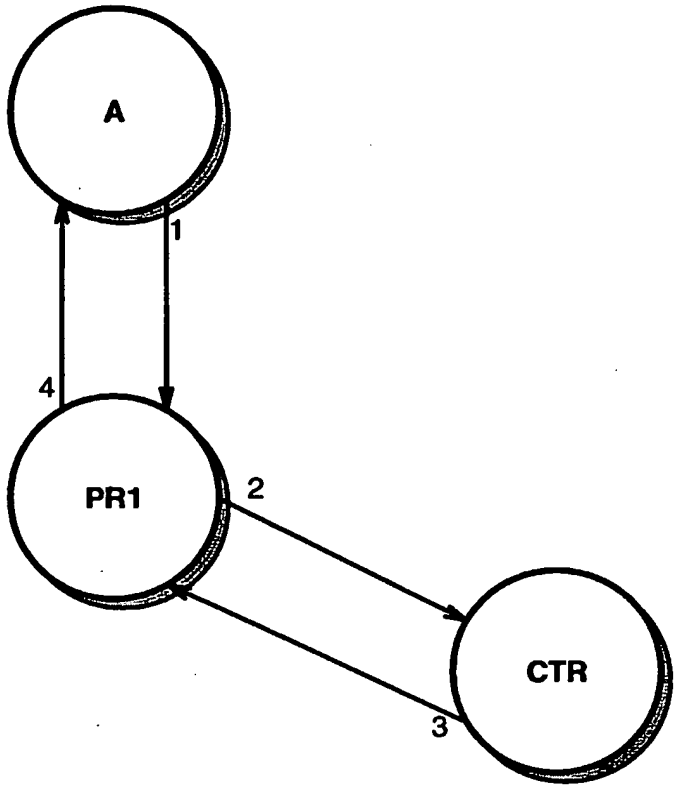


FIG. 2

Field	Description
PIN	Random number issued to purse by purse register to initiate registration process.
Date	Date and time that the purse was registered with the purse register.
Purse ID	Unique code that is used to identify this purse.
Purse Holder ID	Identifies the purse holder.
Status	Flag indicating status of purse.
Subscriber Authorisation Key	Secret key shared between the purse and its purse register.
Expiry Date	The date on which the subscriber authorisation key ceases to be valid.

FIG. 3

Field	Description
Mint's unique ID	Identifies the mint that minted the token
Token register's ID	IP Address of the server holding the token
Issue number	Used by the TR to identify all tokens in an issue
Token's serial number	Identifies the token
Valid from date	YY-MM-DD
Expiry date	YY-MM-DD
Token type	Pence, cents, etc.
Value of token	Number of units 1 to 65535
Escrow date	The date until which the token will be held in escrow
Owner's ID	The ID of the purse to which the token currently belongs
Owner's address	The address of the purse register with which the owner's purse is registered

FIG. 4

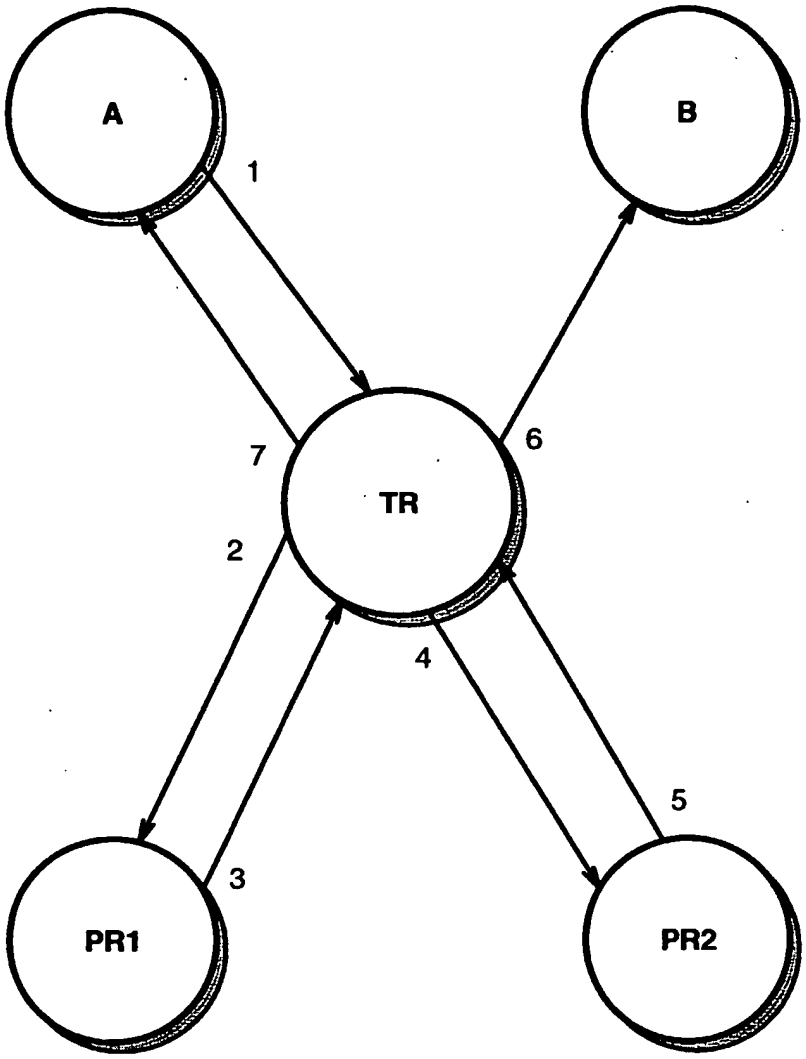


FIG. 5

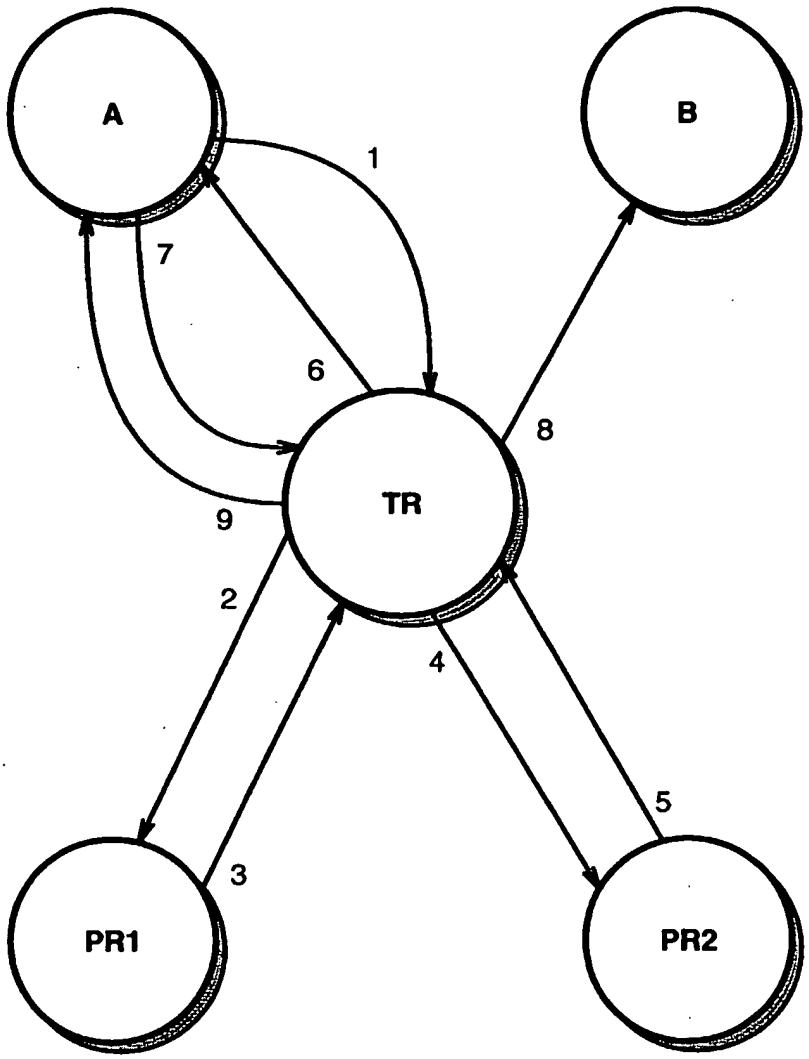


FIG. 6

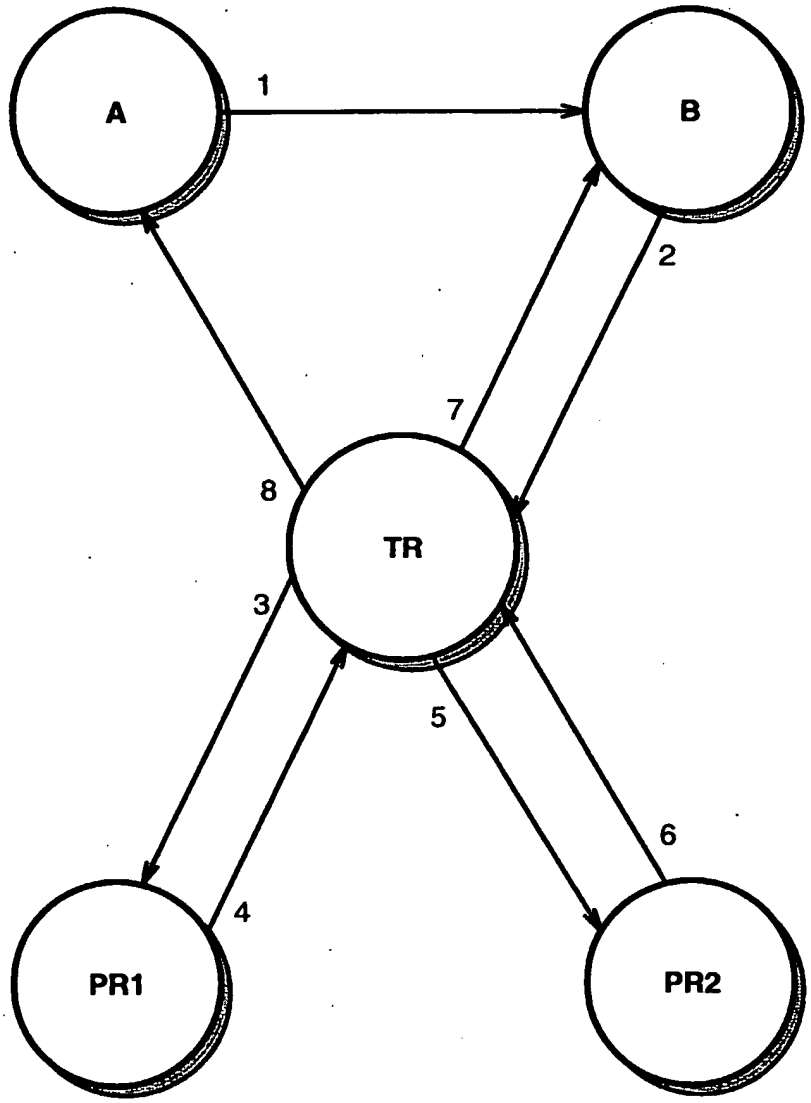


FIG. 7

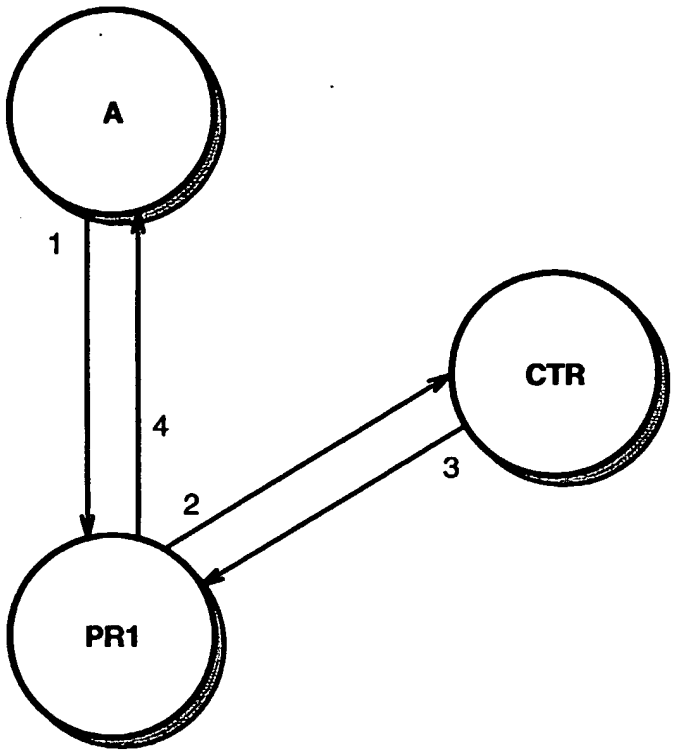


FIG. 8